PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-018469

(43)Date of publication of application : 17.01.1997

---

(51)Int.Cl. H04L 9/16

H04L 9/22

---

(21)Application number : 07-165932 (71)Applicant : CANON INC

(22)Date of filing : 30.06.1995 (72)Inventor : YAMAMOTO TAKAHISA

---

(54) EQUIPMENT AND SYSTEM FOR CIPHER COMMUNICATION AND CIPHERING DEVICE

(57)Abstract:

PURPOSE: To set the proper ciphering system by a transmitter and a receiver in a ciphering communication network.

CONSTITUTION: A terminal 10 for communication is provided with ciphering devices 11 performing ciphering and decoding which are different in ciphering systems, a selection means 14 selecting one of the ciphering devices 11 and a key generation/selector 13 generating the ciphering key according to the selection. The ciphering system which is suitable for the communication is discussed, determined and selected with the terminal 10 for communication on an opposite side. Therefore, the ciphering system having the ciphering intensity according to the secrecy required for information to be communicated is set.

LEGAL STATUS [Date of request for examination] 16.12.1998

[Date of sending the examiner's decision of rejection] 19.06.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] Cryptocommunication equipment equipped with two or more means of communications which perform encryption of transmit data, and decode of reception encryption data, respectively, and communicate mutually, and a selection means to be formed in the above-mentioned means of communications, and to choose one of two or more of the cipher systems.

[Claim 2] Cryptocommunication equipment [equipped with a key generation means to generate the key corresponding to the cipher system which it was prepared in the above-mentioned means of communications, and the above-mentioned selection means chose] according to claim 1.

[Claim 3] Cryptocommunication equipment [equipped with an updating means to make the key which is formed in the above-mentioned means of communications, and is generated with the above-mentioned key generation means at the time of encryption processing of the above-mentioned transmit data update at any time] according to claim 2.

[Claim 4] Cryptocommunication equipment [equipped with a decision means to determine the cipher system which it is prepared in the above-mentioned means of communications, and the above-mentioned selection means chooses by communicating mutually] according to claim 1.

[Claim 5] Cryptocommunication equipment according to claim 2 characterized by using the algorithm of pseudo-random number generation safe in computational

complexity as an algorithm used with the above-mentioned key generation means.

[Claim 6] Cryptocommunication equipment according to claim 5 characterized by using a square mold pseudo-random number generation algorithm as the above-mentioned pseudo-random number generation algorithm safe in computational complexity.

[Claim 7] It is data encryption equipment which is equipped with an encryption means to encipher information, using two or more cipher systems alternatively, and a mode assignment means to specify a mode of operation, and is characterized by the above-mentioned encryption means choosing a cipher system according to the specified mode.

[Claim 8] It is data encryption equipment which is equipped with an encryption means to encipher information, using two or more cipher systems alternatively, and an assignment means to specify a security rank, and is characterized by the above-mentioned encryption means choosing a cipher system according to the specified security rank.

[Claim 9] The cryptocommunication system which is a cryptocommunication system which enabled it to choose a cipher system, and is characterized by needing the consent by the side of the above-mentioned predetermined terminal unit when changing the cipher system specified by the predetermined terminal

unit with other terminal units while communicating the data enciphered among two or more terminals on a network.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the data encryption equipment used for the cryptocommunication equipment, the system, and it which communicate by enciphering data, in order to keep data secret.

[0002]

[Description of the Prior Art] In recent years, exchanging various information using this communication network is going to be realized with maintenance of the optical fiber network in a trunk communication network, the spread of cable television systems, utilization of a health communication link, the spread of local EARI networks, etc. In addition, it considers transmitting multimedia information, such as dynamic-image data, static-image data, voice data, and computer data, as the information. In such a communication network, it is important to transmit information to insurance and various codes are known as a means for it.

Although those codes are roughly divided and it is classified into 2 cipher systems of a common key encryptosystem and public key encryption, various methods are considered to each classification.

[0003] Drawing 14 shows a common key encryptosystem communication network, and drawing 15 shows a public-key-encryption communication network. Drawing 16 shows a common key and public-key-encryption network, and has composition which added the public-key-encryption communication network of drawing 15 to the common key encryptosystem communication network of drawing 14 .

[0004] First, the cryptocommunication by the common key encryption system is described. In the common key encryptosystem communication network, as shown in drawing 14 , the proper and the secret key are beforehand shared among network subscribers. A, B, C, --, M show the subscriber of the network, KAB and KAC, the key that is sharing -- between subscriber A-B, respectively, the key currently shared between subscriber A-C, and --. Furthermore, each subscriber has the terminal for a communication link equipped with the data encryption equipment which enciphers according to the algorithm decided in the network as shown in drawing 17 (and decode). The following procedures perform the common key encryptosystem communication link to B from the conventional subscriber A.

[0005] 1. The secret key KAB currently beforehand shared with the transmission place B is used for A as a key of the data encryption equipment of this communication link, it enciphers correspondence with data encryption equipment, and transmits the enciphered thing to B.

2. B uses the secret key KAB currently shared the transmitting agency A beforehand as a key of the data encryption equipment of this communication link, decodes the receiving sentence from A with data encryption equipment, and obtains correspondence.

[0006] Next, the cryptocommunication by the public key cryptosystem is described. As shown in drawing 15 , each subscriber's public key is put up for the electronic bulletin board of a public-key-encryption communication network in the form where a subscriber's ID (identifier etc.) and correspondence can be taken. It sets to drawing 15 and they are Kp A, Kp B, --, Kp M about Subscribers' A, B, --, M public key. It is shown. Moreover, each subscriber holds secretly the private key corresponding to his own public key. It sets to drawing 15 and they are Ks A and Ks B about Subscribers' A, B, --, M private key. -- Ks M It is shown. Furthermore, each subscriber has the terminal for a communication link equipped with the data encryption equipment which enciphers according to the algorithm decided in the network as shown in drawing 17 (and decode). The following procedures perform the public-key-encryption communication link to B

from the conventional subscriber A.

[0007] Open 1.A of B is the public key Kp B of the transmission place B from the conventional subscriber A. It uses as a key of the data encryption equipment of this communication link, correspondence is enciphered with data encryption equipment, and the enciphered thing is transmitted to B.

2. B is its own private key Kp B. It uses as a key of the data encryption equipment of this communication link, the receiving sentence from A is decoded with data encryption equipment, and correspondence is obtained. Cryptocommunication is performed by these procedures.

[0008] Various methods are considered even if it restricts to the typical cipher system now known about the code technique which is a technique required in order to realize a reliable communication link, as stated above. Moreover, various modes used can be considered also with the same cipher system, and various cures are considered so that reinforcement may be further increased to decryption.

[0009] Here, a DES code is briefly explained as a conventional cipher system. In the DES code, encryption and decode are carried out to a unit in a 64-bit data block, and the die length of a key is made into 56 bits (it is 64 bits when a 8-bit parity bit is added). Cryptographic algorithm is based on the transposition type and the substitution type, by repeating 16 steps of processings which combined

such transposition and substitution suitably, stirred the bit pattern of a plaintext and has changed it into the cipher which semantics does not understand. When decoding, the original plaintext is restored by stirring conversely.

[0010] This parameter of a way to stir is specified with a 56-bit key. The number of the candidates of a key is the 56th power (17th power of about 10) individual of 2, and if decode which a key is changed by a unit of 1 time, and checks it is performed to the pair of the cipher which round robin decoded that is, received, and a plaintext, supposing one check will take 500ns (processing speed of 128Mbps), it will become this count about 1000 on the whole.

[0011] In encryption processing of DES, transposition (initial transposition IP) is first performed to a 64-bit plaintext. This initial transposition is immobilization. After the output of this transposition processing passes through 16 steps of complicated encryption processings the middle, finally transposition (last transposition IP-1) is performed. This last transposition is also immobilization.

[0012] 32 bits is divided into each right and left, and, for a left half, L0 and a right half are [the data which are 64 bits to which initial transposition was performed] R0. It becomes. this L0 R0 from -- processing shown in drawing 18 over 16 steps is performed until it is set to L16 and R16. That is, they are Ln and Rn, respectively about 32 bits of the right and left when ending the n-th step of processing. They are Ln and Rn if it carries out. It is expressed with a degree

type.

[0013] Ln =Rn-1Rn =Ln-1 #f(Rn-1 ,Kn)

[0014] Here, # means the exclusive OR of mod2 for every bit, and is Kn. The 48-bit key inputted into the n-th step, and Ln-1 Rn-1 The n-1st step of output and f are Rn-1, respectively. Kn It is the function which uses and outputs 32-bit data.

[0015]

[Problem(s) to be Solved by the Invention] However, in the conventional cryptocommunication, it was not taken into consideration about adjustment whether to perform cryptocommunication using the method which used which cipher system and mode used by the transmitting side and the receiving side, and took what kind of measures to decryption. Therefore, when it had data encryption equipment which can perform two or more cipher systems by the transmitting person and the addressee, or when two or more modes used were able to be performed, detecting the common cipher system of performing cryptocommunication by adjusting among transceiver persons how or both, and performing cryptocommunication with the cipher system was not completed.

[0016] Furthermore, according to the class of information to exchange, it was not taken into consideration about adjustment of arranging a cipher system by the transmitting side and the receiving side. It was not taken into consideration about adjusting the reinforcement of a code according to the class of information

exchanged especially. For example, when the information to exchange was the high information on confidentiality, cryptocommunication with high safety was performed using the method coped with to decryption which was stated by the Prior art, and when the information to exchange was not the high information on confidentiality, mitigating the load of data encryption equipment was not completed by using the usual cipher system. There were the above problems in the conventional cryptocommunication.

[0017] This invention was accomplished in order to solve the above-mentioned trouble, and it aims at obtaining the cryptocommunication equipment, the system, and data encryption equipment which can choose a cipher system.

[0018]

[Means for Solving the Problem] In invention of claim 1, encryption of transmit data and decode of reception encryption data were performed, respectively, and two or more means of communications which communicate mutually, and a selection means to be formed in the above-mentioned means of communications, and to choose one of two or more of the cipher systems are established.

[0019] In invention of claim 7, it has an encryption means to encipher information, using two or more cipher systems alternatively, and a mode assignment means to specify a mode of operation, and the above-mentioned encryption means

chooses a cipher system according to the specified mode.

[0020] In invention of claim 8, it has an encryption means to encipher information, using two or more cipher systems alternatively, and an assignment means to specify a security rank, and the above-mentioned encryption means chooses a cipher system according to the specified security rank.

[0021] In invention of claim 9, while communicating the data enciphered among two or more terminals on a network, it is the cryptocommunication system which enabled it to choose a cipher system, and when changing the cipher system specified by the predetermined terminal unit with other terminal units, the consent by the side of the above-mentioned predetermined terminal unit is needed.

[0022]

[Function] While being able to set a cipher system as arbitration by establishing the selection means which can choose a cipher system as the means of communications which the transceiver person who performs cryptocommunication uses according to this invention, by sharing the set-up cipher system among transceiver persons in advance of transmission of a cipher, selection of the cipher system which was not conventionally taken into consideration is enabled, and cryptocommunication with a high degree of freedom is made possible. Moreover, selection of code reinforcement is also

enabled.

[0023]

[Example] Although examples 1-8 are shown below, each example is realized from a viewpoint as shown below.

[Example 1] A cipher system is set up out of two or more codes.

[Example 2] A cipher system is set up out of a common key encryptosystem and public key encryption.

[Example 3] A cipher system is set up out of two or more block ciphers.

[Example 4] A cipher system is set up by preparing two or more f functions and choosing them to a DES mold code.

[0024] [Example 5] A cipher system is set up out of the mode used to a block cipher.

[Example 6] A cipher system is set up out of two or more cipher systems "which encipher while updating a key."

[Example 7] A cipher system is set up to a block cipher out of the cipher system "which enciphers using the key of immobilization", and the cipher system "which enciphers while updating a key."

[Example 8] Read-out of the internal variable of the key generation and the selecting arrangement of the cipher system "it enciphers while updating a key" is made possible. [of an example 7]

[0025] However, the essence of this invention is to have a means to choose so that a specific cipher system can be performed out of two or more cipher systems. Moreover, it is in having enabled it to choose the reinforcement of a code by it. Therefore, as two or more cipher systems chosen, it is not limited to the cipher system shown in the example. Although the Prior art also described, since many cipher systems by which the current proposal is made exist, it is difficult to show all those cipher systems in the example. Moreover, a cipher system which combined two or more cipher systems is also contained as a cipher system chosen by this invention.

[0026] In [example 1] this example, as shown in drawing 1 , cryptocommunication is performed using the terminal 10 for a communication link equipped with two or more data encryption equipment 11 which enciphers (and decode), the communication interface 12, key generation and a selecting arrangement 13, and a selection means 14 to choose one from the outputs of two or more data encryption equipment 11.

[0027] Each data encryption equipment 11 realizes processing of a cipher system different, respectively. At this example, it is - cipher system 1 and cipher system 2- as a cipher system. -- It considers as t kinds of codes of the - cipher system t, and suppose that the processing is realized by data encryption equipment 1, data encryption equipment 2, --, each data encryption equipment

11 of data encryption equipment t, respectively. Furthermore, it can set up which data encryption equipment 11 is used with a cipher system setting signal. In addition, in the following explanation, the need is accepted in data encryption equipment 11, and it is data encryption equipment 1. -- It shall be referred to as t.

[0028] The selection means 14 is controlled by the cipher system setting signal, and can be chosen one from the outputs of two or more data encryption equipment 11. For example, what is necessary is just to set up the selection means 14 with a cipher system setting signal, to perform cipher processing of a cipher system 1 so that the output from data encryption equipment 1 may be chosen. What is necessary is just to set up the selection means 14 with a cipher system setting signal, to perform cipher processing of a cipher system 2 similarly so that the output from data encryption equipment 2 may be chosen.

[0029] A communication interface 12 is a communication interface for receiving the transmitting sentence enciphered with the information which shows the cipher system from a communications partner, and data encryption equipment 11 from a transmission line while transmitting the transmitting sentence enciphered with the information which shows a cipher system, and data encryption equipment 11 to a transmission line.

[0030] Furthermore, generally, since the die length of a key differs for every cipher system, with the key generation and the selecting arrangement 13 which

has key generation and a selecting arrangement 13 as a means to generate or choose the key corresponding to the cipher system chosen by the cipher system setting signal, the key corresponding to the cipher system chosen from one key with a certain die length is generated. Or the key with which only the number of cipher systems beforehand realizable [with data encryption equipment] corresponds is prepared, and the key corresponding to the selected cipher system is chosen.

[0031] An example of the key generation and the selecting arrangement 13 by this invention is shown in drawing 2 . Key generation and a selecting arrangement 13 generate a key according to an algorithm as shown below. One key with a certain die length inputted into key generation and a selecting arrangement 13 is used as initial value (x0) with the following algorithms.

$x_{i+1} = f(x_i)$ $(i = 0, 1, --)$ ..... (1)

$b_{i+1} = g(x_{i+1})$ $(i = 0, 1, --)$ ..... (2)

[0032] Key generation and a selecting arrangement 13 consist of computing-element 13c which changes it into a key, when the output of die length required for the key corresponding to processing circuit 13a which performs the feedback operation of a formula (1), processing circuit 13b which performs the operation of a formula (2), and the cipher system chosen by the cipher system setting signal is taken out from the processing circuit 13b which

calculates a formula (2), as shown in drawing 2 .

[0033] b1, b2, --, bi which are outputted in computing-element 13c from processing circuit 13b which calculates a formula (2) It performs changing into the key of the die length corresponding to the cipher system chosen by the cipher system setting signal. A key is the bit string of the die length defined with the algorithm of the selected cipher system, and is b1, and b2, --, bi by computing-element 13c. It is generated arranging as it is or by standing in a line and changing the sequence.

[0034] Therefore, actuation of key generation and a selecting arrangement 13 is as follows.

1. It is x0 as initial value. It inputs into key generation and a selecting arrangement 13.

2. By the formula (1), they are x1, x2, --, xi. It generates.

3. x1 generated, x2, --, xi b1 obtained by receiving and performing a formula (2), and b2, --, bi It outputs.

4. They are b1, and b2, --, bi by computing-element 13c. It outputs as a key corresponding to the cipher system chosen by the cipher system setting signal.

[0035] Key generation and a selecting arrangement 13 generate a key with the die length corresponding to the cipher system which it was controlled by the cipher system setting signal how many times the operation of a formula (1) and a

formula (2) is performed or the key of the die length of which is further outputted from computing-element 13c, and was chosen by that with the cipher system setting signal.

[0036] Moreover, key generation and a selecting arrangement 13 can also be constituted like drawing 3 . Key generation and the selecting arrangement 13 of drawing 3 consist of t keys (k1, and k2, --, kt) and 13d of key selection means. A key k1, and k2, --, kt It is inputted into 13d of key selection means, and either is chosen by the cipher system setting signal. A key with the die length corresponding to the cipher system chosen by the cipher system setting signal by this is chosen.

[0037] The thing of drawing 14 is used as a cryptocommunication network which performs cryptocommunication using the above-mentioned terminal 10 for a communication link. Beforehand, a network manager etc. can realize sharing of a key, when the key sets up. Or it is realizable with a well-known key share method reference "a code and information SEKIRYUTI" (Tsujii, the Kasahara work, the 1990 issue, **** [Co.], Inc., 72-73, 97 to 104 term) As shown.

[0038] Cryptocommunication from the subscriber A by this invention to B is performed by the following procedures. In the following explanation, it supposes that it is what is shown in drawing 2 as key generation and a selecting arrangement 13, and the key corresponding to the cipher system chosen from

one key with a certain die length as mentioned above is generated.

[0039] [The pre-procedure 1 of the cryptocommunication by this invention]

1. The transmitting person A sends the information which shows a cipher system to Addressee B through a communication interface 12.

2. Addressee B receives the information which shows the cipher system sent by the transmitting person A through the information communication interface 12, checks that the data encryption equipment 11 in the terminal 10 for a communication link which Addressee B uses can process with the cipher system, and tells the transmitting person A comprehension of initiation of cryptocommunication through a communication interface 12. When it is difficult to process with the cipher system, a possible cipher system is told to the transmitting person A through a communication interface 12.

3. Repeat until agreement can perform the above-mentioned procedure about a cipher system among transceiver persons.

[0040] Although the above-mentioned pre-procedure 1 showed the information which shows a cipher system from transmitting persons, being conversely shown from addressees as follows is also possible.

[The pre-procedure 2 of the cryptocommunication by this invention]

1. Addressee B sends the information which shows the cipher system when enciphering the demand and information on informational offer to the

transmitting person A through a communication interface 12.

2. The transmitting person A receives the information which shows a demand and cipher system of offer of the information sent by Addressee B through the information communication interface 12, checks that the data encryption equipment in the terminal 10 for a communication link which the transmitting person A uses can process with the cipher system, and tells Addressee B comprehension of initiation of cryptocommunication through a communication interface 12. When it is difficult to process with the cipher system, a possible cipher system is told to Addressee B through a communication interface 12.

3. Repeat until agreement can perform the above-mentioned procedure about a cipher system among transceiver persons.

[0041] The upper procedure is an effective procedure, when a transmitting person does not know the cipher system which can set up a receiving side, or when an addressee does not know the cipher system which can set up a transmitting side. When the transmitting person knows the cipher system which can be set up by the receiving side, or when the addressee knows the cipher system which can set up a transmitting side, it is possible to perform the above-mentioned procedure 1 and **** and to start the next cryptocommunication.

[0042] Furthermore, in a cryptocommunication network which holds a key share

method which exchanges cryptographic keys among transceiver persons in advance of cryptocommunication, it is possible in a key shared protocol to also share the information on a cipher system with the information for sharing of a key. In such a case, it is possible to skip the above-mentioned procedure and to start cryptocommunication.

[0043] According to the procedures 1 and 2 before the above, a cipher system can be adjusted among transceiver persons. Moreover, it is not necessary to perform the procedures 1 and 2 before the above for every communication link each time. For example, it is unnecessary, when the cipher system is beforehand arranged among transceiver persons and the cipher system performs cryptocommunication.

[0044] Hereafter, the following procedure is continued between the transmitting person A and Addressee B.

[The cryptocommunication procedure of the data based on this invention (related with the transmitting person A)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedures 1 and 2 may be chosen by the cipher system setting signal.

2. Set the secret key KAB currently beforehand shared with Addressee B as initial value as the key generation and the selecting arrangement 13 within the

terminal 10 for a communication link, and generate the key corresponding to the cipher system chosen by the cipher system setting signal. The generated key is set as data encryption equipment 11.

3. Encipher data with data encryption equipment 11, choose the cipher outputted from the data encryption equipment 11 determined in the pre-procedure with the selection means 14, and transmit to B through a communication interface 12.

[0045] [The cryptocommunication procedure of the data based on this invention (related with Addressee B)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedures 1 and 2 may be chosen by the cipher system setting signal.

2. Set the secret key KAB currently beforehand shared with the transmitting person A as initial value as the key generation and the selecting arrangement 14 within the terminal 10 for a communication link, and generate the key corresponding to the cipher system chosen by the cipher system setting signal. The generated key is set as data encryption equipment 11.

3. Receive encryption data from a transmission line through a communication interface 12, decode the encryption data sent from A with data encryption equipment 11, and choose the plaintext outputted from the data encryption equipment 11 determined in the pre-procedure with the selection means 14.

[0046] Moreover, it is also possible to use the thing of drawing 3 as key generation and a selecting arrangement 13. In that case, the key shown in drawing 14 means what set two or more keys. that is, the key KAB2 when using the key KAB1 in case a cipher system 1 is used for the key KAB between Subscribers A and B, and a cipher system 2, --, the key KABt when using a cipher system t from -- it becomes. Cryptocommunication from the subscriber A by this invention in this case to B is performed by the following procedures. However, since it is the same as the above, the pre-procedures 1 and 2 are skipped.

[0047] [The cryptocommunication procedure of the data based on this invention (related with the transmitting person A)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedure may be chosen by the cipher system setting signal.

2. the secret key KAB (it consists of KAB [1], KAB [2], --, KABt) currently beforehand shared with Addressee B -- the key generation and the selecting arrangement 13 within the terminal 10 for a communication link -- setting up -- a cipher system setting signal -- two or more keys KAB1, KAB2, --, KABt from -- the key corresponding to the selected cipher system is chosen. The selected key is set as data encryption equipment 11.

3. Encipher data with data encryption equipment 11, choose the cipher outputted from the data encryption equipment 11 determined in the pre-procedure with the selection means 14, and transmit to B through a communication interface 12.

[0048] [The cryptocommunication procedure of the data based on this invention (related with Addressee B)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedure may be chosen by the cipher system setting signal.

2. the secret key KAB (it consists of KAB [1], KAB [2], --, KABt) currently beforehand shared with the transmitting person A -- the key generation and the selecting arrangement 13 within the terminal 10 for a communication link -- setting up -- a cipher system setting signal -- two or more keys KAB1, KAB2, --, KABt from -- the key corresponding to the selected cipher system is chosen. The selected key is set as data encryption equipment 11.

3. Receive encryption data from a transmission line through a communication interface 12, decode the encryption data sent from A with data encryption equipment 11, and choose the plaintext outputted from the data encryption equipment 11 determined in the pre-procedure with the selection means 14.

[0049] Moreover, since confidential information, such as a key of each user required in order to carry out cryptocommunication, is stored, the subscriber of a

cryptocommunication network may hold the pocket mold storage 30 as shown in drawing 4 , respectively. The confidential information of each user required in order to carry out cryptocommunication is stored in the pocket mold storage 30, and it is made a configuration which has the pocket mold storage 30 for every user independently [the terminal 10 for a communication link] in consideration of safety. Although the pocket mold storage 30 may be some terminals 10 for a communication link if a safe field is physically securable for every user, the terminal 10 for a communication link which can be used for cryptocommunication for every user in that case will be restricted. In separating the terminal 10 for a communication link, and the pocket mold storage 30, and making it not store each user's confidential information in the terminal 10 for a communication link, a user becomes possible [exchanging the user's confidential information through its own pocket mold storage 30, and using it for cryptocommunication at every terminal 10 for a communication link,], and is convenience.

[0050] The pocket mold storage 30 can exchange information now through the above-mentioned terminal for a communication link, and a safe channel, and has a safe field as maintenance means 30a physically. It is only the owner of normal that the pocket mold storage 30 can be operated normally, and it judges whether you are the owner of normal in authentication procedure, such as a password. Moreover, the thing related to the owner of the pocket mold storage

30 is held to maintenance means 30a among the above-mentioned share keys. The pocket mold storage 30 is realizable with an IC card etc. In all the examples 2-8 explained below, it is the range of this invention also about the case where this pocket mold storage 30 is used.

[0051] In [example 2] this example, cryptocommunication is performed using the terminal 10 for a communication link equipped with two or more data encryption equipment 15 and 16 which performs encryption (and decode) as shown in drawing 5 , the communication interface 12, key generation and a selecting arrangement 13, and a selection means 14 to choose one from the outputs of two or more data encryption equipment 15 and 16.

[0052] At this example, it is a DES cipher system (or FEAL cipher system) considering a cipher system as a representative of 1. common key encryption system.

2. It shall consider as two kinds of cipher systems of RSA encryption technology (or ElGamal cryptosystem method) as a representative of a public key cryptosystem, and the processing shall be realized by DES data encryption equipment (or FEAL data encryption equipment) 15 and RSA data encryption equipment (or ElGamal cryptosystem equipment) 16, respectively. However, the DES code illustrated here, a FEAL code, RSA cryptograph, and an ElGamal cryptosystem were only mentioned as an example of representation of a

common key encryptosystem or public key encryption, and this invention is not limited to these but can be applied to other cryptographic algorithms.

[0053] What is necessary is just to choose the output from DES data encryption equipment 15 with the selection means 14, in using the terminal 10 for a communication link of drawing 5 with a DES cipher system. What is necessary is just to choose the output from RSA data encryption equipment 16 with the selection means 14, in using the terminal 10 for a communication link of drawing 5 by RSA encryption technology.

[0054] The same thing as an example 1 is used for key generation and a selecting arrangement 13, a communication interface 12, and the selection means 14. However, key generation and a selecting arrangement 13 choose the key corresponding to the cipher system chosen by the cipher system setting signal using what was shown in drawing 3 . That is, when the key beforehand distributed to DES codes when a DES cipher system is chosen is chosen and RSA encryption technology is chosen, the public key currently opened to RSA cryptograph is chosen.

[0055] Moreover, in this example, the thing of drawing 16 is used as a cryptocommunication network. The common key of drawing 16 and the public-key-encryption communication network have composition in which drawing 15 carried out public-key-encryption communication network addition in

the common key encryptosystem communication network of drawing 14 .

[0056] Cryptocommunication from the subscriber A by this invention to B is performed by the following procedures. However, the pre-procedures 1 and 2 are the same as that of an example 1.

[The cryptocommunication procedure of the data based on this invention (related with the transmitting person A)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedure may be chosen by the cipher system setting signal.

2. a cipher system setting signal -- the common key KAB and public key Kp B from -- the key corresponding to the selected cipher system is chosen. The selected key is set as data encryption equipment 15 and 16.

3. Encipher data with data encryption equipment 15 and 16, choose the cipher outputted from the data encryption equipment determined in the pre-procedure with the selection means 14, and transmit to B through a communication interface 12.

[0057] [The cryptocommunication procedure of the data based on this invention (related with Addressee B)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedure may be chosen by the cipher system setting

signal.

2. a cipher system setting signal -- the common key KAB and public key Ks B from -- the key corresponding to the selected cipher system is chosen. The selected key is set as data encryption equipment 15 and 16.

3. Receive encryption data from a transmission line through a communication interface 12, decode the encryption data sent from A with data encryption equipment, and choose the plaintext outputted from the data encryption equipment determined in the pre-procedure with the selection means 14.

[0058] With this procedure, it can adjust about a cipher system among transceiver persons, and the safety of cryptocommunication can be chosen. That is, a cipher system can be chosen according to the confidentiality of data which transmits. For example, in the case of the high data of especially confidentiality, a public key cryptosystem is chosen, when that is not right, a common key encryption system is chosen and processing is simplified. What says can be performed.

[0059] In [example 3] this example, cryptocommunication is performed using the terminal 10 for a communication link equipped with two or more data encryption equipment 17 and 18 which performs encryption (and decode) as shown in drawing 6 , the communication interface 12, key generation and a selecting arrangement 13, and a selection means 14 to choose one from the outputs of

two or more data encryption equipment 17 and 18.

[0060] At this example, it is a 1.DES code as a cipher system.

2. FEAL Code

It shall consider as the block cipher of two kinds of **, and the processing shall be realized by DES data encryption equipment 17 and FEAL data encryption equipment 18, respectively. However, the DES code and FEAL code which were illustrated here were only mentioned as an example of representation of a common key encryptosystem, and this invention is not limited to these but can apply other cryptographic algorithms.

[0061] What is necessary is just to always choose the output from DES data encryption equipment 17 with the selection means 14 to perform DES cipher processing using the terminal 10 for a communication link of drawing 6 . Moreover, what is necessary is just to always choose the output from FEAL data encryption equipment 18 with the selection means 14 to perform FEAL cipher processing.

[0062] The same thing as an example 1 is used for key generation and a selecting arrangement 13, a communication interface 12, and the selection means 14. Moreover, the thing of drawing 14 is used as a cryptocommunication network which performs cryptocommunication using the above-mentioned terminal 10 for a communication link. And cryptocommunication from the

subscriber A by this example to B is performed by the same procedure as an example 1.

[0063] In [example 4] this example, cryptocommunication is performed using the terminal 10 for a communication link equipped with the data encryption equipment 19 which performs encryption (and decode) as shown in drawing 7 , the communication interface 12, and key generation and a selecting arrangement 13. Moreover, the selection means 14 used in the old examples 1-3 is included in data encryption equipment 19 by this example.

[0064] In this example, a DES mold (in BORYUSHON mold) code is used as a cipher system. Two or more cipher systems can be set up by preparing two or more f functions which are the component, and choosing a certain f function from the inside. Since a DES mold code is an algorithm which repeats the same processing as mentioned above, it can perform repeat processing in the same circuit. For example, if it circuit-izes as one batch for one step of the DES code shown in drawing 18 , cipher processing is realizable by repeating and using the circuit.

[0065] The data encryption equipment 19 in this case is constituted like drawing 8 . The data encryption equipment 19 of drawing 8 consists of 19d of selection means to choose one from the output of Registers 19a and 19b, exclusive "or" circuit 19c, two or more f functions (f1, and f2, --, ft), and two or more f functions.

19d of selection means is controlled by the cipher system setting signal.

[0066] The configuration of two or more f functions is realizable by preparing the group of Sbox of the same number for example, as f function. In this case, f function f1 It receives and is S11, S12, --, S18. Sbox is used and it is the f function f2. What is necessary is to receive and just to make it call it -- using Sbox of S21, S22, --, S28. Moreover, f function f1 It receives, f function of a DES code is used, and it is the f function f2. It is realizable also by preparing f function of a completely different code like [it receives and] -- using f function of a FEAL code.

[0067] It is possible to perform cryptocommunication with the same procedure as an example 1 using data encryption equipment 19 which was explained above. In addition, the same thing as an example 1 is used for key generation and a selecting arrangement 13, and a communication interface 12. This example also uses the thing of drawing 14 as a cryptocommunication network. This example can adjust a cipher system among transceiver persons.

[0068] In [example 5] this example, cryptocommunication is performed using the terminal for a communication link of the same configuration as the terminal 10 for a communication link shown in drawing 7 . However, data encryption equipment 20 as replaced with the data encryption equipment 19 of drawing 7 and shown in drawing 9 is used. Moreover, as for the selection means, this example is also

contained in data encryption equipment 20. Moreover, since the bit length of a key does not change with a cipher system, key generation and a selecting arrangement 13 are not necessarily required of this example.

[0069] By this example, a block cipher is considered as a cipher system. Furthermore, it shall set up with a cipher system setting signal by which of 1.ECB (Electric Codebook) mode 2.CBC (Cipher Block Chaining) mode, using the block cipher.

[0070] Although later mentioned about the CBC mode, it explains briefly also here. It is DK about EK and decode in the encryption set [a plaintext] Ci and initial value to IV for Mi and a cipher, and using the cryptographic key K. The CBC mode is expressed with a degree type when it carries out.

C1 =EK (M1+IV) ..... (3)

Ci =EK (i(Mi+Ci-1) = 2, 3, --) ..... (4)

M1 =DK+(C1) IV ..... (5)

Mi =DK+(Ci) Ci-1 (i= 2, 3, --) ..... (6)

[0071] The data encryption equipment 20 in this case is constituted like drawing 9 . The data encryption equipment 20 of drawing 9 consists of block cipher machine 20a, selection means 20b which chooses one side from two inputs, and exclusive "or" circuit 20c which performs EXCLUSIVE OR operation for every bit. Selection means 20b is controlled by the cipher system setting signal.

[0072] What is necessary is to make all into the bit string of 0 as initial value IV to input, and just to always choose initial value IV in selection means 20b, in using this data encryption equipment 20 in ECB mode. Moreover, what is necessary is to set up the bit string of arbitration as initial value IV to input, to choose initial value IV, when enciphering an early block, and just to choose the output from data encryption equipment 20 in selection means 20b, henceforth, in using data encryption equipment 20 in the CBC mode. It is not necessary to make initial value IV secret among operators.

[0073] It is possible to perform cryptocommunication with the same procedure as an example 1 using data encryption equipment 20 which was explained above. However, in a pre-procedure, when the CBC mode is chosen, the procedure of sharing initial value IV is needed. For example, before performing cryptocommunication, the procedure of transmitting initial value IV to B from A is needed. Since it is not necessary to make initial value IV secret among transceiver persons, it is not necessary to encipher. Moreover, not only the secret key KAB but the shared initial value IV must be set as the data encryption equipment 20 within the terminal 10 for a communication link.

[0074] Key generation and the selecting arrangement 13 communication interface 12 use the same thing as an example 1. This example also uses the thing of drawing 14 as a cryptocommunication network. This example can adjust

the mode used of a cipher system among transceiver persons.

[0075] [Example 6] this example improves a cipher system based on an example 1. In this example, cryptocommunication is performed as well as an example 1 using the terminal 10 for a communication link shown in drawing 1 .

[0076] The point that this example differs from an example 1 is as follows. Although two or more data encryption equipment 11 existed in the example 1, the key to each data encryption equipment 11 is immobilization while performing cryptocommunication once. That is, during cryptocommunication, a key is not necessarily changed at any time, and the same key is used from the start of cryptocommunication to an end. In order to raise safety to decryption by the 3rd person by this example to it, a key is changed at any time during cryptocommunication. In order to update a key at any time during cryptocommunication, whenever the key of the die length corresponding to the cipher system as which under cryptocommunication performed key generation and was chosen by the cipher system setting signal is generated, the key of data encryption equipment 11 is updated with key generation and a selecting arrangement 13. However, it is necessary to perform renewal of a key by taking a synchronization by the transmitting person and addressee of cryptocommunication.

[0077] Key generation and the selecting arrangement 13 of this example are

also constituted like [it is the same with the case of an example 1, and] drawing 2 . However, in key generation and the selecting arrangement 13 of this example, whenever the key of the die length corresponding to the cipher system as which under cryptocommunication performed key generation and was chosen by the cipher system setting signal as mentioned above is generated, in order to perform updating the key of data encryption equipment 11, the case and actuation of an example 1 differ from each other.

[0078] If the key of the die length corresponding to the cipher system chosen by the cipher system setting signal is generated, it is not necessary to operate the key generation and the selecting arrangement 13 in the case of an example 1 more than it. It is necessary to generate the key of the die length corresponding to the cipher system chosen by the cipher system setting signal one after another to it with the key generation and the selecting arrangement 13 in this example. That is, the key generation and the selecting arrangement 13 in this example repeat repeatedly actuation of the key generation and the selecting arrangement 13 in the case of an example 1, and is performing it.

[0079] Although especially the algorithm of key generation of the key generation and the selecting arrangement 13 used for this invention can use a general thing as not necessarily received a limit and shown in the example 1, when a pseudo-random number sequence generation algorithm safe in computational

complexity is used as an algorithm of key generation, by this example, the case where a square mold pseudo-random number sequence is especially used also in it is explained.

[0080] Square mold pseudo-random number sequences are the pseudo-random number sequence b1 generated in the following procedures, b2, and --.

[Square mold pseudo-random number sequence] p and q are made into the prime factor which is p**q**3 (mod4), and they are initial value x0 (1<x 0 < N-1 integer) and a recursive type as N=p-q. xi+1 =xi 2 modN (i= 0, 1 and 2, --) ..... (7)

bi =lsbj (i(xi) = 1, 2, --) ..... (8)

The bit sequence b1 acquired as be alike, b2, and -- are called square mold pseudo-random number sequence. However, lsbj (xi) is xi. j bits of low order are expressed, and when the number of bits of N is set to n, it considers as j=O (log2 n).

[0081] a square pseudo-random number sequence -- law -- the judgment problem of the quadratic residue nature in N serves as a pseudo-random number sequence safe in computational complexity under assumption that it is difficult in computational complexity. in order to make a square pseudo-random number sufficiently safe -- the law of square operation expression (7) -- it is desirable to make number-of-bits n of N into about 512 bits. furthermore, Keys

(initial value of key generation and a selecting arrangement) KAB and KAC and -- which are beforehand shared secretly among each subscriber -- 1 -- < -- KAB, KAC, and -- < -- it is referred to as N-1.

[0082] The key generation and the selecting arrangement 13 using this square pseudo-random number sequence are shown in drawing 10 . Key generation and the selecting arrangement 13 of drawing 10 consist of 13f of processing circuits and 13g of arithmetic units which perform the operation of processing circuit 13e which performs the feedback operation of a formula (7), and a formula (8). Actuation of this key generation and selecting arrangement 13 is as follows.

1. Initial value x0 It inputs into key generation and a selecting arrangement 13.

2. A formula (7) generates x1, x2, and --.

3. To x1 generated, x2, and --, perform a formula (8) and output b1 obtained, b2, and --.

4. Change b1, b2, and -- into the string key k1 of the key of the die length corresponding to the cipher system chosen by the cipher system setting signal, k2, and -- in 13g of computing elements.

[0083] Drawing of the cryptocommunication in the case of updating a key at any time to drawing 11 is shown. A block cipher is considered as a cipher system. Setting to drawing 11 , for ku (u= 1, 2, --, t), ku (u(Muv) = 1, 2, --, t;v= 1, 2, --, s) is

[Muv (u= 1, 2, --, t;v= 1, 2, --, s) / block / plaintext] Key ku about the plaintext block Muv in the key of a block cipher. The cipher block enciphered and acquired is shown. Here, s blocks from Mu1 to Mus are the same keys ku. It is enciphered. The plaintext block of drawing 11 is enciphered by two or more cryptographic keys by using in order the key sequence k1 updated by above-mentioned key generation and selecting arrangement 13, k2, and -- as a key of a block cipher. Thus, by updating a key at any time, the number of the plaintext blocks enciphered with the same key becomes s pieces, and can make analysis of a key difficult. In addition, this example also uses the thing of drawing 14 as a cryptocommunication network.

[0084] Cryptocommunication from Subscriber A to B is performed by the following procedures. However, the pre-procedure is the same as that of an example 1.

[The cryptocommunication procedure of the data based on this invention (related with the transmitting person A)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedure may be chosen by the cipher system setting signal.

2. Set the secret key KAB currently beforehand shared with Addressee B as initial value as the key generation and the selecting arrangement 13 within the

terminal 10 for a communication link, and generate the string key corresponding to the cipher system chosen by the cipher system setting signal.

3. It uses updating the string key outputted from key generation and a selecting arrangement 13 at any time as a key of data encryption equipment 11, encipher data, choose the cipher outputted from the data encryption equipment 11 determined in the pre-procedure with the selection means 14, and transmit to B through a communication interface 12.

[0085] [The cryptocommunication procedure of the data based on this invention (related with Addressee B)]

1. Set up the selection means 14 so that the output from the cipher system determined in the pre-procedure may be chosen by the cipher system setting signal.

2. Set the secret key KAB currently beforehand shared with the transmitting person A as initial value as the key generation and the selecting arrangement 13 within the terminal 10 for a communication link, and generate the string key corresponding to the cipher system chosen by the cipher system setting signal.

3. Encryption data are received from a transmission line through a communication interface 12, and use, updating the string key outputted from key generation and a selecting arrangement 13 at any time as a key of data encryption equipment 11, decode the sent encryption data, and choose the

plaintext outputted from the data encryption equipment 11 determined in the pre-procedure with the selection means 14.

[0086] Moreover, although the square mold pseudo-random number was used as an algorithm of pseudo-random number generation safe in computational complexity, anythings can be used if it is a pseudo-random number generation algorithm safe in computational complexity. for example, it is shown in said reference "a code and an information security" (Tsujii, the Kasahara work, the 1990 issue, **** [Co.], Inc., 86 pages) -- as -- RSA cryptograph and dispersion -- the thing using a logarithm and an inverse number code can also be used for the algorithm of pseudo-random number generation of this invention. Moreover, the approach of updating the key explained by this example at any time is not only applicable to an example 1 but applicable to examples 3, 4, and 5, although explained based on the example 1.

[0087] As for the [example 7] example 1, a key chooses a certain cipher system from the cipher systems (plurality) of immobilization, and an example 6 chooses a certain cipher system from the cipher systems (plurality) with which a key is updated. The key enables it to choose a cipher system by this example as a variation of the two above-mentioned examples 1 and 6 between the cipher systems with which the cipher system and key of immobilization are updated. Moreover, in this example, cryptocommunication is performed using the data

encryption equipment 11 which performs encryption (and decode) as shown in drawing 12 , a communication interface 12, and the terminal 10 for a communication link equipped with key generation and a selecting arrangement 13. Here, since explanation is easy, data encryption equipment 11 presupposes that it is one.

[0088] By this example, a block cipher is considered as a cipher system. Furthermore, the block cipher is enciphered using the key of 1. immobilization.

2. Encipher, updating a key.

It shall set up with a cipher system setting signal, using *******'s and others method.

[0089] Key generation and a selecting arrangement 13 are controlled by the cipher system setting signal, and in using it with the cipher system "which enciphers using the key of immobilization", key generation and a selecting arrangement 13 will suspend processing, if a fixed key (one key) is generated. Moreover, in using it with" cipher system which enciphers while updating a key, it performs actuation of repeating processing and performing it in order that key generation and a selecting arrangement 13 may generate a string key (two or more keys). What is necessary is for a cipher system setting signal to generate a fixed key in key generation and a selecting arrangement 13, and just to encipher using the fixed key in data encryption equipment 11, in using the terminal 10 for

a communication link of drawing 12 with the cipher system "which enciphers using the key of immobilization." Moreover, what is necessary is for a cipher system setting signal to generate a string key in key generation and a selecting arrangement 13, and just to encipher in data encryption equipment 11, updating a key one by one with the string key, in using the terminal 10 for a communication link of drawing 12 with the cipher system "which enciphers while updating a key." Key generation and a selecting arrangement 13 use what has actuation the same as an example 6 with the same configuration as drawing 2 . Data encryption equipment 11 and a communication interface 12 use the same thing as an example 1. Moreover, the thing of drawing 14 is used as a cryptocommunication network.

[0090] Cryptocommunication from Subscriber A to B is performed by the same procedure as an example 1. However, when enciphering updating a key is chosen, the cryptocommunication procedure of data is performed by the same procedure as an example 6.

[0091] By this example, it can adjust about a cipher system among transceiver persons, and the safety of cryptocommunication can be chosen. That is, a cipher system can be chosen according to the confidentiality of data which transmits. For example, in the case of the high data of especially confidentiality, it can perform choosing the cipher system "which enciphers while updating a key",

choosing the cipher system "which enciphers using the key of immobilization", and simplifying processing, when that is not right. In addition, although data encryption equipment 11 was set to one in this example since explanation was easy, two or more data encryption equipment 11 may be used. In that case, the selection means 14 for choosing the output from two or more data encryption equipment 11 is needed.

[0092] [Example 8] this example is the case where a little configuration of the key generation and the selecting arrangement 13 used in the examples 6 and 7 is changed. In the examples 6 and 7, since the key currently shared among each subscriber is immobilization, when a transceiver person is the same, the initial value of key generation and a selecting arrangement 13 turns into the always same value, and has the problem that the same string key is generated, also in the cipher system "which enciphers while updating a key."

[0093] then, even when a transceiver person is the same, whenever he uses the initial value of key generation and a selecting arrangement 13, as he changes, he is trying to raise safety in this example

[0094] xi+1 updated one after another by the feedback operation in the formula (7) and formula (8) which are the procedure of the string key generation shown in the example 6 It will be called the internal variable of key generation and a selecting arrangement 13. Key generation and the selecting arrangement 13 of

this example consist of 13h of processing circuits which perform the feedback operation of a formula (7), processing circuit 13i which performs the operation of a formula (8), and computing-element 13j, as shown in drawing 13 , and it has composition which can read the internal variable further updated by the operation of a formula (7). The read internal variable is memorized by maintenance means 30a of the pocket mold storage 30 connected to the terminal 10 for a communication link which was explained in the example 1.

[0095] Although migration of data is an one direction only by setting initial value to key generation and a selecting arrangement 13 in the examples 6 and 7, in this example, the internal variable of key generation and a selecting arrangement 13 can be read to hard flow. Replacement is performed to the common key which used the read internal variable for this cryptocommunication as a common key used for next cryptocommunication.

[0096] Moreover, the terminal 10 for a communication link which can be changed whenever it uses the initial value of key generation and a selecting arrangement 13 can be constituted by transposing this key generation and selecting arrangement 13 to key generation and the selecting arrangement 13 of drawing 10 .

[0097] Cryptocommunication from Subscriber A to B is performed by the procedure shown in the examples 6 and 7, and the same procedure. However,

in the case of the cipher system "which enciphers while updating a key", the procedure of "holding secretly as new initial value for carrying out cryptocommunication to A (or B) next time the value of the internal variable of a key generation and a selecting arrangement when decode of encryption data is completed to the maintenance means of pocket mold storage" to both transceiver person is needed at the end.

[0098] Each above-mentioned example is constituted so that it may be based on the cipher system setting signal, it may shift and that cipher system may be used alternatively. A transmitting person may choose an above-mentioned cipher system setting signal as arbitration, and you may make it choose one of cipher systems automatically here according to the class of data transmitted. Furthermore, when a transmitting person specifies the security rank of transmitting contents, you may make it set up automatically the cipher system which has the reinforcement according to the specified security rank. Moreover, you may make it the above-mentioned cipher system setting signal change code reinforcement automatically according to the mode in which the communication link between the modes of operation A and B between the transmitting persons A and B, i.e., transmitting persons, holds for example, TV meeting, the mode in which a confidential communication link is performed, etc. Furthermore, those who communicate data may set up a setup of the above-mentioned cipher

system preferentially, and may enable it to set it up to both the transmitting person freely. However, when weakening code reinforcement, it is desirable to perform the communication link which performs negotiation for needing the other party's consent and obtaining the consent. Furthermore, you may make it set up a cipher system according to the decode capacity of the other party.

[0099]

[Effect of the Invention] As explained above, by establishing the selection means which can choose a cipher system as the means of communications which the transceiver person who performs cryptocommunication uses, by enabling it to change a cipher system and sharing the selected cipher system among transceiver persons in advance of transmission of a cipher further, selection of the conventionally impossible cipher system is enabled and, according to this invention, cryptocommunication with a high degree of freedom is made possible.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram of the terminal for a communication link by the examples 1 and 6 of this invention.

[Drawing 2] It is the block diagram of the key generation and the selecting arrangement by the examples 1, 6, and 7 of this invention.

[Drawing 3] It is the block diagram of other key generation and selecting arrangements by the example 1 of this invention.

[Drawing 4] It is the block diagram of the pocket mold store by the examples 1-8 of this invention.

[Drawing 5] It is the block diagram of the terminal for a communication link by the example 2 of this invention.

[Drawing 6] It is the block diagram of the terminal for a communication link by the example 3 of this invention.

[Drawing 7] It is the block diagram of the terminal for a communication link by the example 4 of this invention.

[Drawing 8] It is the block diagram of the data encryption equipment by the example 4 of this invention.

[Drawing 9] It is the block diagram of the data encryption equipment by the example 5 of this invention.

[Drawing 10] It is the block diagram of the key generation and the selecting arrangement using the square mold pseudo-random number by the example 6 of this invention.

[Drawing 11] It is a block diagram for explaining the cryptocommunication in the

case of performing renewal of a key by the example 6 of this invention.

[Drawing 12] It is the block diagram of the terminal for a communication link by the example 7 of this invention.

[Drawing 13] It is the block diagram of the key generation and the selecting arrangement using the square mold pseudo-random number by the example 8 of this invention.

[Drawing 14] It is the block diagram of a common key encryptosystem communication network.

[Drawing 15] It is the block diagram of a public-key-encryption communication network.

[Drawing 16] It is the block diagram of a common key and public-key-encryption communication network.

[Drawing 17] It is the block diagram of the conventional terminal for a communication link.

[Drawing 18] It is the block diagram showing processing for one step of a DES code.

[Description of Notations]

10 Communication Terminal

11-20 Data encryption equipment

12 Communication Interface

13 Key Generation and Selecting Arrangement

14 Selection Means

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－18469

(43)公開日　平成９年(1997)１月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３	
	9/22					６５５	C5-6

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願平7－165932

(22)出願日　平成７年(1995)６月30日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　山本　貴久
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

(74)代理人　弁理士　國分　孝悦

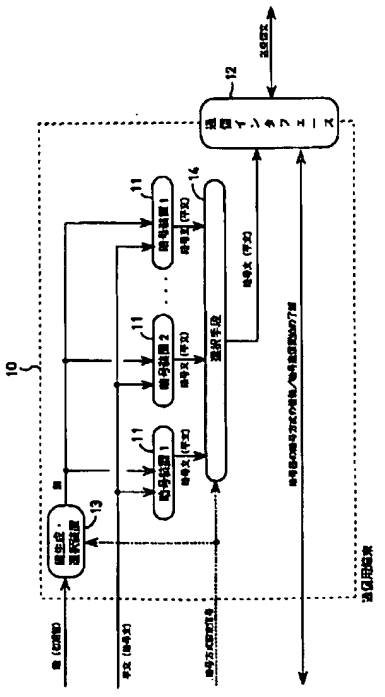
(54)【発明の名称】　暗号通信装置、システム及び暗号装置

(57)【要約】

【目的】　暗号通信ネットワークにおいて送受信者が適切な暗号方式を設定できるようにする。

【構成】　通信用端末１０には、それぞれ暗号方式の異る暗号化及び復号を行う暗号装置１１、暗号装置１１の１つを選択する選択手段１４、その選択に応じて暗号の鍵を生成する鍵生成・選択装置１３が設けられ、相手側の通信用端末１０とその通信に適した暗号方式を互いに打合わせをして決定し、選択できるようにする。

【効果】　通信する情報に要求される機密性に応じた暗号強度を有する暗号方式を設定することができる。



1

【特許請求の範囲】

【請求項１】　それぞれ送信データの暗号化及び受信暗号化データの復号を行い、互いに通信を行う複数の通信手段と、

上記通信手段に設けられ、複数の暗号化方式の１つを選択する選択手段とを備えた暗号通信装置。

【請求項２】　上記通信手段に設けられ、上記選択手段が選択した暗号化方式に対応した鍵を生成する鍵生成手段を備えた請求項１記載の暗号通信装置。

【請求項３】　上記通信手段に設けられ、上記送信データの暗号化処理時に上記鍵生成手段で生成される鍵を随時更新させる更新手段を備えた請求項２記載の暗号通信装置。

【請求項４】　上記通信手段に設けられ、上記選択手段が選択する暗号化方式を、互いに通信を行うことにより決定する決定手段を備えた請求項１記載の暗号通信装置。

【請求項５】　上記鍵生成手段で用いるアルゴリズムとして、計算量的に安全な疑似乱数生成のアルゴリズムを用いることを特徴とする請求項２記載の暗号通信装置。

【請求項６】　上記計算量的に安全な疑似乱数生成アルゴリズムとして２乗型疑似乱数生成アルゴリズムを用いることを特徴とする請求項５記載の暗号通信装置。

【請求項７】　複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、

動作モードを指定するモード指定手段とを備え、

上記暗号化手段は、指定されたモードに応じて暗号化方式を選択することを特徴とする暗号装置。

【請求項８】　複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、

セキュリティランクを指定する指定手段とを備え、

上記暗号化手段は、指定されたセキュリティランクに応じて暗号化方式を選択することを特徴とする暗号装置。

【請求項９】　ネットワーク上の複数端末間で暗号化されたデータの通信を行うとともに、暗号化方式を選択し得るようにした暗号通信システムであって、

所定の端末装置により指定された暗号化方式を他の端末装置により変更する場合に、上記所定の端末装置側の承諾を必要とすることを特徴とする暗号通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データを秘匿するためにデータを暗号化して通信を行う暗号通信装置、システム及びそれに用いる暗号装置に関するものである。

【０００２】

【従来の技術】近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛生通信の実用化、ローカルエアリネットワークの普及等に伴い、かかる通信網を利用して様々な情報をやり取りすることが実現されようとしている。加えて、その情報

2

として動画像データ、静止画像データ、音声データ、コンピュータデータ等のマルチメディア情報を伝送することが考えられている。このような通信網においては、情報を安全に伝達することが重要であり、そのための手段として種々の暗号が知られている。それらの暗号は大きく分けて、共通鍵暗号と公開鍵暗号との２つ暗号方式に分類されるが、それぞれの分類に対して種々の方式が考えられている。

【０００３】図１４は共通鍵暗号通信ネットワーク、図１５は公開鍵暗号通信ネットワークを示す。図１６は共通鍵、公開鍵暗号ネットワークを示し、図１４の共通鍵暗号通信ネットワークに図１５の公開鍵暗号通信ネットワークを付加した構成になっている。

【０００４】まず、共通鍵暗号方式による暗号通信について述べる。共通鍵暗号通信ネットワークでは、図１４に示すように、あらかじめネットワークの加入者間で固有かつ秘密の鍵を共有している。A、B、C、…、Mはそのネットワークの加入者、K_{AB}、K_{AC}、…はそれぞれ加入者A－B間で共有している鍵、加入者A－C間で共有している鍵、…を示している。さらにそれぞれの加入者は、図１７に示すような、ネットワークで決められたアルゴリズムに従って暗号化（及び復号）を行う暗号装置を備えた通信用端末を持っている。従来の加入者AからBへの共通鍵暗号通信は以下の手順で行う。

【０００５】１．Aは、あらかじめ送信先Bと共有している秘密の鍵K_{AB}を本通信の暗号装置の鍵として用いて暗号装置により通信文を暗号化し、その暗号化したものをBに送信する。

２．Bはあらかじめ送信元Aと共有している秘密の鍵K_{AB}を本通信の暗号装置の鍵として用いて暗号装置によりAからの受信文を復号し、通信文を得る。

【０００６】次に、公開鍵暗号方式による暗号通信について述べる。図１５に示すように、公開鍵暗号通信ネットワークの電子掲示板には、各加入者の公開鍵が加入者のＩＤ（名前等）と対応がとれる形で掲示されている。図１５においては、加入者A、B、…、Mの公開鍵をK^P_A、K^P_B、…、K^P_Mで示している。また各加入者は自分の公開鍵に対応した秘密鍵を秘密に保有する。図１５においては、加入者A、B、…、Mの秘密鍵をK^S_A、K^S_B、…、K^S_Mで示している。さらにそれぞれの加入者は、図１７に示されるような、ネットワークで決められたアルゴリズムに従って暗号化（及び復号）を行う暗号装置を備えた通信用端末を持っている。従来の加入者AからBへの公開鍵暗号通信は以下の手順で行う。

【０００７】従来の加入者AからBの公開

１．Aは送信先Bの公開鍵K^P_Bを本通信の暗号装置の鍵として用いて暗号装置により通信文を暗号化し、その暗号化したものをBに送信する。

２．Bは、自分の秘密鍵K^P_Bを本通信の暗号装置の鍵

として用いて暗号装置によりAからの受信文を復号し、通信文を得る。これらの手順により暗号通信が行われる。

【0008】以上述べたように、信頼できる通信を実現するために必要な技術である暗号技術に関し、現在のところ知られている代表的な暗号方式に限っても種々の方式が考えられている。また、同じ暗号方式でもいろいろな使用モードが考えられており、さらに暗号解読に対して強度を増すように、いろいろな対策が考えられている。

【0009】ここで、従来の暗号方式としてDES暗号について簡単に説明する。DES暗号では、64ビットのデータブロックを単位に暗号化及び復号が行われ、鍵の長さは56ビット（8ビットのパリティビットを加えると64ビット）とされている。暗号アルゴリズムは転置式と換字式とを基本としており、これらの転置と換字を適当に組み合わせた処理を16段繰り返すことにより、平文のビットパターンをかき混ぜ、意味の分からない暗号文に変換している。復号する場合は、逆にかき混ぜることにより、元の平文を復元する。

【0010】このかき混ぜかたのパラメータを56ビットの鍵で指定する。鍵の候補の数は2の56乗（約10の17乗）個であり、総当たりの解読、つまり入手した暗号文と平文のペアに対し、鍵を1回ずつ変化させてチェックする解読を行うと、1回のチェックに500nsかかるとすると（128Mbpsの処理速度）、全体で1000年程度かかる計算になる。

【0011】DESの暗号化処理では、まず64ビットの平文に対して転置（初期転置IP）が行われる。この初期転置は固定である。この転置処理の出力は途中複雑な16段の暗号化処理を経た後に最後に転置（最終転置IP^{-1}）が行われる。この最終転置も固定である。

【0012】初期転置が行われた64ビットのデータは、32ビットずつ左右に分割され左半分がL_0、右半分がR_0となる。このL_0とR_0からL_{16}とR_{16}になるまで16段にわたって図18に示す処理が行われる。つまり、n段目の処理を終了したときの左右の32ビットをそれぞれL_n、R_nとすると、L_n、R_nは次式で表されるものとなる。

【0013】$L_n = R_{n-1}$

$R_n = L_{n-1} \# f(R_{n-1}, K_n)$

【0014】ここで、#はビット毎のmod2の排他的論理和を意味し、K_nはn段目に入力される48ビットの鍵、L_{n-1}とR_{n-1}はそれぞれn－1段目の出力、fはR_{n-1}とK_nを用いて32ビットのデータを出力する関数である。

【0015】

【発明が解決しようとする課題】しかしながら、従来の暗号通信においては、送信側と受信側でどの暗号方式や使用モードを使用し、また暗号解読に対してどのような対策を施した方式を使用して暗号通信を行うのかという調整に関しては考慮されていなかった。そのため、送信者と受信者で複数の暗号方式を実行できる暗号装置を持つ場合や、複数の使用モードが実行できる場合に、どのようにして送受信者間で調整を行うことにより、暗号通信を行うのか、あるいは両者の共通の暗号方式を検知して、その暗号方式により暗号通信を行う、というようなことができなかった。

【0016】さらに、やり取りする情報の種類に応じて、送信側と受信側とで暗号方式を打ち合わせるなどの調整に関しては考慮されていなかった。特に、やり取りする情報の種類に応じて暗号の強度を調整することに関しては考慮されてなかった。例えば、やり取りする情報が機密性の高い情報であれば従来の技術で述べたような暗号解読に対し対策を施した方式を用いて安全性の高い暗号通信を行い、やり取りする情報が機密性の高い情報でなければ、通常の暗号方式を用いることにより、暗号装置の負荷を軽減する、というようなことができなかった。従来の暗号通信においては、以上のような問題があった。

【0017】本発明は、上記の問題点を解決するために成されたもので、暗号方式を選択できる暗号通信装置、システム及び暗号装置を得ることを目的としている。

【0018】

【課題を解決するための手段】請求項1の発明においては、それぞれ送信データの暗号化及び受信暗号化データの復号を行い、互いに通信を行う複数の通信手段と、上記通信手段に設けられ、複数の暗号化方式の1つを選択する選択手段とを設けている。

【0019】請求項7の発明においては、複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、動作モードを指定するモード指定手段とを備え、上記暗号化手段は、指定されたモードに応じて暗号化方式を選択する。

【0020】請求項8の発明においては、複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、セキュリティランクを指定する指定手段とを備え、上記暗号化手段は、指定されたセキュリティランクに応じて暗号化方式を選択する。

【0021】請求項9の発明においては、ネットワーク上の複数端末間で暗号化されたデータの通信を行うとともに、暗号化方式を選択し得るようにした暗号通信システムであって、所定の端末装置により指定された暗号化方式を他の端末装置により変更する場合に、上記所定の端末装置側の承諾を必要とする。

【0022】

【作用】本発明によれば、暗号通信を行う送受信者の利用する通信手段に、暗号方式を選択できる選択手段を設けることにより、暗号方式を任意に設定できると共に、その設定した暗号方式を暗号文の送信に先立って送受信

5

者間で共有することにより、従来考慮されていなかった暗号方式の選択を可能にし、自由度の高い暗号通信を可能にしている。また、暗号強度の選択も可能にしている。

【0023】

【実施例】以下に実施例1～8を示すが、各実施例は次に示すような観点から成り立っている。

［実施例1］　複数の暗号の中から暗号方式を設定する。

［実施例2］　共通鍵暗号と公開鍵暗号の中から暗号方式を設定する。

［実施例3］　複数のブロック暗号の中から暗号方式を設定する。

［実施例4］　ＤＥＳ型暗号に対し、複数のｆ関数を用意し、それらを選択することにより、暗号方式を設定する。

【0024】［実施例5］　ブロック暗号に対し、使用モードの中から暗号方式を設定する。

［実施例6］　「鍵を更新しながら暗号化を行う」複数の暗号方式の中から暗号方式を設定する。

［実施例7］　ブロック暗号に対し、「固定の鍵を用いて暗号化を行う」暗号方式と、「鍵を更新しながら暗号化を行う」暗号方式の中から暗号方式を設定する。

［実施例8］　実施例7の「鍵を更新しながら暗号化を行う」暗号方式の鍵生成・選択装置の内部変数を読み出し可能にする。

【0025】ただし、本発明の本質は、複数の暗号方式の中から特定の暗号方式を実行できるように選択する手段を有することにある。また、それによって暗号の強度を選択できるようにしたことにある。従って、選択される複数の暗号方式としては、実施例に示した暗号方式に限定されるものではない。従来の技術でも述べたが、現在提案されている暗号方式は多数存在するため、その全ての暗号方式について実施例で示すことは困難である。また、複数の暗号方式を組み合わせたような暗号方式も、本発明により選択される暗号方式として含まれる。

【0026】［実施例1］本実施例では、図1に示すように、暗号化（及び復号）を行う複数の暗号装置１１と、通信インタフエース１２と、鍵生成・選択装置１３と、複数の暗号装置１１の出力の中から１つを選択する選択手段１４とを備えた通信用端末１０を用いて暗号通＊

6

＊信を行う。

【0027】各々の暗号装置１１は、それぞれ異なる暗号方式の処理を実現する。本実施例では暗号方式として、

・暗号方式1
・暗号方式2
・…
・暗号方式t

のｔ種類の暗号とし、それぞれ暗号装置1、暗号装置2、…、暗号装置ｔの各暗号装置１１でその処理が実現されているとする。さらに、どの暗号装置１１を使用するかを暗号方式設定信号により設定できる。尚、以下の説明では、暗号装置１１を必要に応じて暗号装置1…ｔと呼ぶものとする。

【0028】選択手段１４は、暗号方式設定信号によって制御され、複数の暗号装置１１の出力の中から1つ選択することができる。例えば、暗号方式1の暗号処理を行いたい場合には、暗号方式設定信号によって選択手段１４を暗号装置1からの出力を選択するように設定すればよい。同様に暗号方式2の暗号処理を行いたい場合には暗号方式設定信号によって選択手段１４を暗号装置2からの出力を選択するように設定すればよい。

【0029】通信インタフェース１２は、暗号方式を示す情報と暗号装置１１で暗号化された送信文とを伝送路に送信するとともに、通信相手からの暗号方式を示す情報と暗号装置１１で暗号化された送信文とを伝送路から受信するための通信インタフェースである。

【0030】さらに、一般に暗号方式毎に鍵の長さは異なっているため、暗号方式設定信号によって選択された暗号方式に対応した鍵を生成、または選択する手段として鍵生成・選択装置１３がある、鍵生成・選択装置１３では、ある長さを持つ1つの鍵から選択された暗号方式に対応した鍵を生成する。あるいはあらかじめ暗号装置で実現できる暗号方式の数だけ対応する鍵を用意しておき、選択された暗号方式に対応した鍵を選択する。

【0031】図2に本発明による鍵生成・選択装置１３の一例を示す。鍵生成・選択装置１３は、次に示すようなアルゴリズムに従って鍵を生成する。鍵生成・選択装置1.3に入力されるある長さを持つ1つの鍵は、以下のアルゴリズムで初期値（x_0）として用いられる。

$$x_{i+1} = f(x_i) \quad (i=0, 1, \cdots) \qquad \cdots\cdots\cdots (1)$$

$$b_{i+1} = g(x_{i+1}) \quad (i=0, 1, \cdots) \qquad \cdots\cdots\cdots (2)$$

【0032】鍵生成・選択装置１３は、図2に示すように、式（1）のフィードバック演算を行う処理回路１３ａと、式（2）の演算を行う処理回路１３ｂと、暗号方式設定信号で選択された暗号方式に対応した鍵に必要な長さの出力が、式（2）の演算を行う処理回路１３ｂから出されたときにそれを鍵に変換する演算器１３ｃとから構成される。

【0033】演算器１３ｃでは、式（2）の演算を行う処理回路１３ｂから出力されるb_1、b_2、…、b_lを暗号方式設定信号で選択された暗号方式に対応した長さの鍵に変換することを行う。鍵は選択された暗号方式のアルゴリズムで定められた長さのビット列であり、演算器１３ｃによって例えばb_1、b_2、…、b_lをそのまま並べることにより、あるいはその順序を並び変えるこ

とにより生成される。

【００３４】従って、鍵生成・選択装置１３の動作は以下のようになる。

１．初期値としてx_0を、鍵生成・選択装置１３に入力する。

２．式（１）により、x_1、x_2、…、x_tを生成する。

３．生成されたx_1、x_2、…、x_tに対して式（２）を実行し、得られたb_1、b_2、…、b_tを出力する。

４．演算器１３ｃによりb_1、b_2、…、b_tを暗号方式設定信号で選択された暗号方式に対応した鍵として出力する。

【００３５】鍵生成・選択装置１３は、暗号方式設定信号によって、式（１）及び式（２）の演算を何回行うか、さらに演算器１３ｃからどれだけの長さの鍵を出力するか、を制御され、そのことにより暗号方式設定信号によって選択された暗号方式に対応した長さを持つ鍵を生成する。

【００３６】また、鍵生成・選択装置１３は図３のように構成することも可能である。図３の鍵生成・選択装置１３はｔ個の鍵（k_1、k_2、…、k_t）と鍵選択手段１３ｄとから構成される。鍵k_1、k_2、…、k_tは鍵選択手段１３ｄに入力され、暗号方式設定信号によっていずれかが選択される。これにより暗号方式設定信号によって選択された暗号方式に対応した長さを持つ鍵を選択する。

【００３７】上記通信用端末１０を用いて暗号通信を行う暗号通信ネットワークとしては図１４のものを用いる。鍵の共有は、あらかじめネットワークの管理者等が鍵の設定しておくことによって実現できる。あるいは、文献「暗号と情報セキリュティ」（辻井、笠原著、１９９０年発行、株式会社昭晃社、７２～７３、９７～１０４項）示されるような公知の鍵共有方式によっても実現できる。

【００３８】本発明による加入者ＡからＢへの暗号通信は以下の手順で行われる。以下の説明では、鍵生成・選択装置１３としては、図２に示すものであるとし、上記のように、ある長さを持つ１つの鍵から選択された暗号方式に対応した鍵を生成する。

【００３９】［本発明による暗号通信の前手順１］

１．送信者Ａは、暗号方式を示す情報を通信インタフェース１２を介して受信者Ｂに送る。

２．受信者Ｂは、送信者Ａから送られてきた暗号方式を示す情報を情報通信インタフェース１２を介して受信し、受信者Ｂが利用している通信用端末１０にある暗号装置１１がその暗号方式で処理できることを確認し、暗号通信の開始の了解を通信インタフェース１２を介して送信者Ａに伝える。その暗号方式で処理することが困難な場合には、可能な暗号方式を通信インタフェース１２を介して送信者Ａに伝える。

３．上記手順を送受信者間で暗号方式に関して合意ができるまで繰り返す。

【００４０】上記の前手順１では、暗号方式を示す情報を送信者の方から示したが、逆に次のように受信者の方から示すことも可能である。

［本発明による暗号通信の前手順２］

１．受信者Ｂは、情報の提供の要求とその情報を暗号化する時の暗号方式を示す情報を通信インタフェース１２を介して送信者Ａに送る。

２．送信者Ａは、受信者Ｂから送られてきた情報の提供の要求と暗号方式を示す情報とを情報通信インタフェース１２を介して受信し、送信者Ａが利用している通信用端末１０にある暗号装置がその暗号方式で処理できることを確認し、暗号通信の開始の了解を通信インタフェース１２を介して受信者Ｂに伝える。その暗号方式で処理することが困難な場合には、可能な暗号方式を通信インタフェース１２を介して受信者Ｂに伝える。

３．上記手順を送受信者間で暗号方式に関して合意ができるまで繰り返す。

【００４１】上の手順は送信者が受信側の設定可能な暗号方式を知らない場合、あるいは受信者が送信側の設定可能な暗号方式を知らない場合に有効な手順である。送信者が受信側で設定可能な暗号方式を知っている場合、又は受信者が送信側の設定可能な暗号方式を知っている場合には、上記の手順１、だけを行って次の暗号通信を開始することが可能である。

【００４２】さらに、暗号通信に先立って暗号鍵を送受信者間で交換するような鍵共有方式を行うような暗号通信ネットワークにおいては、鍵共有のプロトコルにおいて、鍵の共有のための情報と共に暗号方式の情報も共有することが可能である。そのような場合には、上記の手順を省略して暗号通信を開始することが可能である。

【００４３】上記前手順１、２によれば、送受信者間で暗号方式を調整することができる。また、上記前手順１、２は通信毎に毎回行う必要はない。例えば、あらかじめ暗号方式を送受信者間で打ち合わせておき、その暗号方式で暗号通信を行う場合には必要ない。

【００４４】以下、送信者Ａと受信者Ｂとの間で次の手順を続ける。

［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順１、２で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ受信者Ｂと共有している秘密の鍵K_{AB}を通信用端末１０内の鍵生成・選択装置１３に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵を生成する。生成された鍵は暗号装置１１に設定される。

３．暗号装置１１によりデータを暗号化し、選択手段１

４により前手順で決定した暗号装置１１から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００４５】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順１、２で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ送信者Ａと共有している秘密の鍵K_{AB}を通信用端末１０内の鍵生成・選択装置１４に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵を生成する。生成された鍵は暗号装置１１に設定される。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、暗号装置１１によりＡから送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置１１から出力される平文を選択する。

【００４６】また、鍵生成・選択装置１３として図３のものを用いることも可能である。その場合には、図１４に示された鍵は、複数の鍵を合わせたものを意味する。つまり、加入者ＡとＢの間の鍵K_{AB}は、暗号方式１を使う時の鍵K_{AB1}、暗号方式２を使う時の鍵K_{AB2}、…、暗号方式ｔを使う時の鍵K_{ABt}からなる。この場合の本発明による加入者ＡからＢへの暗号通信は以下の手順で行われる。ただし、前手順１、２は上記と同じなので省略する。

【００４７】［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ受信者Ｂと共有している秘密の鍵K_{AB}（K_{AB1}、K_{AB2}、…、K_{ABt}から構成される）を通信用端末１０内の鍵生成・選択装置１３に設定し、暗号方式設定信号により、複数の鍵K_{AB1}、K_{AB2}、…、K_{ABt}から選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１１に設定される。

３．暗号装置１１によりデータを暗号化し、選択手段１４により前手順で決定した暗号装置１１から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００４８】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ送信者Ａと共有している秘密の鍵K_{AB}（K_{AB1}、K_{AB2}、…、K_{ABt}から構成される）を通信用端末１０内の鍵生成・選択装置１３に設定し、暗号方式設定信号により、複数の鍵K_{AB1}、K_{AB2}、…、K_{ABt}から選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１１に設定される。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、暗号装置１１によりＡから送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置１１から出力される平文を選択する。

【００４９】また暗号通信ネットワークの加入者はそれぞれ、暗号通信するために必要な各ユーザの鍵などの秘密情報を格納するために、図４に示されるような携帯型記憶装置３０を保有していてもよい。携帯型記憶装置３０には、暗号通信するために必要な各ユーザの秘密情報が格納されており、安全性を考慮して通信用端末１０とは別に各ユーザ毎に携帯型記憶装置３０を持つような構成にしている。各ユーザ毎に物理的に安全な領域が確保できるなら携帯型記憶装置３０は通信用端末１０の一部であってもよいが、その場合は各ユーザ毎に暗号通信に使用できる通信用端末１０が制限されてしまう。通信用端末１０と携帯型記憶装置３０とを分離し、通信用端末１０には各ユーザの秘密情報を格納しないようにすることで、ユーザはどの通信用端末１０でも自分の携帯型記憶装置３０を介してそのユーザの秘密情報をやりとりして暗号通信に使用することが可能となり便利である。

【００５０】携帯型記憶装置３０は、上記通信用端末と安全な通信路を介して情報のやり取りを行えるようになっており、物理的に安全な領域を保持手段３０ａとして持つ。携帯型記憶装置３０を正常に動作させることができるのは正規の所有者だけであり、パスワード等の認証手続きにより正規の所有者か否かを判断する。また、上記の共有鍵のうちその携帯型記憶装置３０の所有者に関係するものを保持手段３０ａに保持している。携帯型記憶装置３０はＩＣカード等により実現できる。以下に説明する全ての実施例２～８において、この携帯型記憶装置３０を用いる場合に関しても本発明の範囲である。

【００５１】［実施例２］本実施例では、図５に示すような、暗号化（及び復号）を行う複数の暗号装置１５、１６と、通信インタフエース１２と、鍵生成・選択装置１３と、複数の暗号装置１５、１６の出力の中から１つを選択する選択手段１４とを備えた通信用端末１０を用いて暗号通信を行う。

【００５２】本実施例では、暗号方式を

１．共通鍵暗号方式の代表としてＤＥＳ暗号方式（またはＦＥＡＬ暗号方式）

２．公開鍵暗号方式の代表としてＲＳＡ暗号方式（またはＥｌＧａｍａｌ暗号方式）の２種類の暗号方式とし、それぞれＤＥＳ暗号装置（またはＦＥＡＬ暗号装置）１５と、ＲＳＡ暗号装置（またはＥｌＧａｍａｌ暗号装置）１６とでその処理が実現されているものとする。ただし、ここで例示したＤＥＳ暗号、ＦＥＡＬ暗号、ＲＳＡ暗号、ＥｌＧａｍａｌ暗号は、共通鍵暗号或は公開鍵暗号の代表例として挙げただけで、本発明はこれらに限

定されず他の暗号アルゴリズムにも適用可能である。

【００５３】図５の通信用端末１０をＤＥＳ暗号方式で使用する場合には、選択手段１４ではＤＥＳ暗号装置１５からの出力を選択するようにすればよい。図５の通信用端末１０をＲＳＡ暗号方式で使用する場合には、選択手段１４ではＲＳＡ暗号装置１６からの出力を選択するようにすればよい。

【００５４】鍵生成・選択装置１３、通信インタフェース１２、選択手段１４は、実施例１と同様のものを用いる。ただし、鍵生成・選択装置１３は図３に示されたものを用い、暗号方式設定信号によって選ばれた暗号方式に対応する鍵を選択する。つまり、ＤＥＳ暗号方式が選ばれた場合は、ＤＥＳ暗号用にあらかじめ配布されている鍵を選択し、ＲＳＡ暗号方式が選ばれた場合は、ＲＳＡ暗号用に公開されている公開鍵を選択する。

【００５５】また、本実施例では、暗号通信ネットワークとしては図１６のものを用いる。図１６の共通鍵、公開鍵暗号通信ネットワークは図１４の共通鍵暗号通信ネットワークに図１５の公開鍵暗号通信ネットワーク付加した構成になっている。

【００５６】本発明による加入者ＡからＢへの暗号通信は、以下の手順で行われる。ただし、前手順１、２は実施例１と同様である。

［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．暗号方式設定信号により、共通鍵K_{AB}と公開鍵K^{p}_{B}とから選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１５、１６に設定される。

３．暗号装置１５、１６によりデータを暗号化し、選択手段１４により前手順で決定した暗号装置から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００５７】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．暗号方式設定信号により、共通鍵K_{AB}と公開鍵K^{s}_{B}とから選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１５、１６に設定される。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、暗号装置によりＡから送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置から出力される平文を選択する。

【００５８】この手順により、送受信者間で暗号方式について調整することができ、暗号通信の安全性を選択することができる。つまり、送信するデータの機密性に応じて暗号方式を選択できる。例えば，特に機密性の高いデータの場合には、公開鍵暗号方式を選択し、そうでない場合には、共通鍵暗号方式を選択して処理を簡易にする。というようなことができる。

【００５９】［実施例３］本実施例では、図６に示されるような、暗号化（及び復号）を行う複数の暗号装置１７、１８と、通信インタフエース１２と、鍵生成・選択装置１３と、複数の暗号装置１７、１８の出力の中から１つを選択する選択手段１４とを備えた通信用端末１０を用いて暗号通信を行う。

【００６０】本実施例では、暗号方式として

１．ＤＥＳ暗号

２．ＦＥＡＬ暗号

の２種類のブロック暗号とし、それぞれＤＥＳ暗号装置１７と、ＦＥＡＬ暗号装置１８とでその処理が実現されるものとする。ただし、ここで例示したＤＥＳ暗号、ＦＥＡＬ暗号は共通鍵暗号の代表例として挙げただけで、本発明はこれらに限定されず他の暗号アルゴリズムも適用可能である。

【００６１】図６の通信用端末１０を用いてＤＥＳ暗号処理を行いたい場合は、選択手段１４では常にＤＥＳ暗号装置１７からの出力を選択するようにすればよい。また、ＦＥＡＬ暗号処理を行いたい場合は、選択手段１４では常にＦＥＡＬ暗号装置１８からの出力を選択するようにすればよい。

【００６２】鍵生成・選択装置１３、通信インタフェース１２、選択手段１４は、実施例１と同様のものを用いる。また、上記通信用端末１０を用いて暗号通信を行う暗号通信ネットワークとしては図１４のものを用いる。そして本実施例による加入者ＡからＢへの暗号通信は実施例１と同様の手順で行われる。

【００６３】［実施例４］本実施例では、図７に示すような、暗号化（及び復号）を行う暗号装置１９と、通信インタフエース１２と、鍵生成・選択装置１３とを備えた通信用端末１０を用いて暗号通信を行う。また、これまでの実施例１～３で用いている選択手段１４は、本実施例では暗号装置１９内に含まれている。

【００６４】本実施例では、暗号方式としてＤＥＳ型（インボリューション型）暗号を用いる。その構成要素であるｆ関数を複数用意し、その中からあるｆ関数を選択することにより、複数の暗号方式を設定できる。ＤＥＳ型暗号は前述したように同じ処理を繰り返すアルゴリズムであるので、同じ回路で繰り返し処理を行うことが可能である。例えば図１８に示されたＤＥＳ暗号の１段分の１処理単位として回路化すれば、その回路を繰り返し用いることにより、暗号処理を実現できる。

【００６５】この場合の暗号装置１９は図８のように構成される。図８の暗号装置１９は、レジスタ１９ａ、１９ｂと、排他的論理和回路１９ｃと、複数のｆ関数（f_1、f_2、…、f_t）と、複数のｆ関数の出力から１つ

を選択する選択手段１９ｄとから構成される。選択手段１９ｄは、暗号方式設定信号によって制御されている。

【００６６】複数のｆ関数の構成は、例えばｆ関数と同じ数のＳｂｏｘの組を用意しておくことにより実現可能である。この場合には、ｆ関数f_1に対してはS_{11}、S_{12}、…、S_{18}のＳｂｏｘを用い、ｆ関数f_2に対してはS_{21}、S_{22}、…、S_{28}のＳｂｏｘを用い、…、というようにすればよい。また、ｆ関数f_1に対してはＤＥＳ暗号のｆ関数を用い、ｆ関数f_2に対してはＦＥＡＬ暗号のｆ関数を用い、…、というように、全く異なる暗号のｆ関数を用意することによっても実現できる。

【００６７】以上説明したような暗号装置１９を用いて、実施例１と同様の手順により暗号通信を行うことが可能である。尚、鍵生成・選択装置１３、通信インタフェース１２は、実施例１と同様のものを用いる。本実施例でも、暗号通信ネットワークとしては図１４のものを用いる。本実施例により、送受信者間で暗号方式について調整することができる。

【００６８】［実施例５］本実施例では、図７に示す通＊信用端末１０と同一構成の通信用端末を用いて暗号通信を行う。ただし、図７の暗号装置１９に代えて図９に示すような暗号装置２０を用いる。また、選択手段は本実施例でも暗号装置２０内に含まれている。また、本実施例では、暗号方式によって鍵のビット長は変わらないので鍵生成・選択装置１３は必ずしも必要ではない。

【００６９】本実施例では、暗号方式としてブロック暗号を考える。さらに、そのブロック暗号を

１．ＥＣＢ（Ｅｌｅｃｔｒｉｃ　Ｃｏｄｅｂｏｏｋ）モード

２．ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モード

のどちらで使用するか暗号方式設定信号により設定できるものとする。

【００７０】ＣＢＣモードについては後述するが、ここでも簡単に説明しておく。平文をM_i、暗号文をC_i、初期値をＩＶとし、暗号鍵Ｋを用いた暗号化をE_K、復号をD_KとするとＣＢＣモードは次式で表される。

$$C_1 = E_K(M_1 + IV) \quad \cdots\cdots (3)$$

$$C_i = E_K(M_i + C_{i-1}) \quad (i = 2, 3, \cdots) \quad \cdots\cdots (4)$$

$$M_1 = D_K(C_1) + IV \quad \cdots\cdots (5)$$

$$M_i = D_K(C_i) + C_{i-1} \quad (i = 2, 3, \cdots) \quad \cdots\cdots (6)$$

【００７１】この場合の暗号装置２０は図９のように構成される。図９の暗号装置２０は、ブロック暗号器２０ａと、２つの入力から一方を選択する選択手段２０ｂと、ビット毎に排他的論理和演算を行う排他的論理和回路２０ｃとからなる。選択手段２０ｂは、暗号方式設定信号によって制御されている。

【００７２】この暗号装置２０をＥＣＢモードで使用する場合には、入力する初期値ＩＶとして全て０のビット列とし、選択手段２０ｂでは常に初期値ＩＶを選択するようにすればよい。また暗号装置２０をＣＢＣモードで使用する場合には、入力する初期値ＩＶとして任意のビット列を設定し、選択手段２０ｂでは初期のブロックを暗号化する時には初期値ＩＶを選択するようにし、以降は暗号装置２０からの出力を選択するようにすればよい。初期値ＩＶは通信者間で秘密にする必要はない。

【００７３】以上説明したような暗号装置２０を用いて、実施例１と同様の手順により暗号通信を行うことが可能である。ただし、前手順において、ＣＢＣモードを選択した場合には、初期値ＩＶを共有する手順が必要となる。例えば、暗号通信を行う前にＡからＢへ初期値ＩＶを送信する手順が必要となる。初期値ＩＶは送受信者間で秘密にする必要はないので、暗号化しなくてもよい。また、秘密の鍵K_{AB}だけでなく、共有した初期値ＩＶを通信用端末１０内の暗号装置２０に設定しなければならない。

【００７４】鍵生成・選択装置１３通信インタフェース１２は実施例１と同じものを用いる。本実施例でも、暗号通信ネットワークとしては図１４のものを用いる。本実施例により、送受信者間で暗号方式の使用モードを調整することができる。

【００７５】［実施例６］本実施例は、実施例１に基づいて暗号方式を改良したものである。本実施例では、実施例１と同じく、図１に示す通信用端末１０を用いて暗号通信を行う。

【００７６】本実施例が実施例１と異なる点は以下の通りである。実施例１では暗号装置１１は複数存在したが、各々の暗号装置１１に対する鍵は一度の暗号通信を行っている間は固定である。つまり、暗号通信中には鍵が随時変更されるということはなく、暗号通信の初めから終わりまで同一の鍵を用いる。それに対して本実施例では、第３者による暗号解読に対して安全性を向上させるために、暗号通信中に鍵を随時変更する。暗号通信中に鍵を随時更新するために、鍵生成・選択装置１３では暗号通信中も鍵生成を行い、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成される毎に、暗号装置１１の鍵の更新を行う。ただし、鍵の更新は暗号通信の送信者と受信者とで同期をとって行う必要がある。

【００７７】本実施例の鍵生成・選択装置１３も、実施例１の場合と同じく図２のように構成される。ただし、本実施例の鍵生成・選択装置１３では上述のように、暗号通信中も鍵生成を行い、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成される毎に、暗号装置１１の鍵の更新をする、ということを行うため、実

施例1の場合と動作が異っている。

【0078】実施例1の場合の鍵生成・選択装置13は、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成されればそれ以上動作させる必要はない。それに対して本実施例での鍵生成・選択装置13では、暗号方式設定信号で選択された暗号方式に対応した長さの鍵を次々に生成する必要がある。つまり、本実施例での鍵生成・選択装置13は、実施例1の場合の鍵生成・選択装置13の動作を何度も繰り返し行っている。

【0079】本発明に用いる鍵生成・選択装置13の鍵生成のアルゴリズムは、特に制限を受ける訳ではなく、＊

$$x_{i+1} = x_i^2 \bmod N \quad (i=0、1、2、\cdots) \qquad \cdots\cdots\cdots (7)$$

$$b_i = lsb_j\ (x_i)\ (i=1、2、\cdots) \qquad \cdots\cdots\cdots (8)$$

によって得られるビット系列b_1、b_2、…を2乗型疑似乱数系列という。但し、$lsb_j\ (x_i)$はx_iの下位jビットを表わし、Nのビット数をnとしたときj＝O（$\log_2 n$）とする。

【0081】2乗疑似乱数系列は、法Nにおける平方剰余性の判定問題が計算量的に困難であるとの仮定の下で計算量的に安全な疑似乱数系列となる。2乗疑似乱数を十分安全なものとするため、2乗演算式（7）の法Nのビット数nを512ビット程度とすることが望ましい。さらに、各加入者間であらかじめ秘密に共有されている鍵（鍵生成・選択装置の初期値）K_{AB}、K_{AC}、…は、1＜K_{AB}、K_{AC}、…＜N－1とする。

【0082】この2乗疑似乱数系列を用いた鍵生成・選択装置13は図10に示される。図10の鍵生成・選択装置13は式（7）のフィードバック演算を行う処理回路13eと式（8）の演算を行う処理回路13fと演算装置13gとから構成される。この鍵生成・選択装置13の動作は以下のようになる。

1．初期値x_0を鍵生成・選択装置13に入力する。

2．式（7）により、x_1、x_2、…を生成する。

3．生成されたx_1、x_2、…に対し、式（8）を実行し、得られたb_1、b_2、…を出力する。

4．演算器13gではb_1、b_2、…を暗号方式設定信号で選択された暗号方式に対応した長さの鍵の鍵列k_1、k_2、…に変換する。

【0083】図11に鍵を随時更新する場合の暗号通信の図を示す。暗号方式としてブロック暗号を考える。図11において、M_{uv}（u＝1、2、…、t；v＝1、2、…、s）は平文ブロックを、k_u（u＝1、2、…、t）はブロック暗号の鍵を、k_u（M_{uv}）（u＝1、2、…、t；v＝1、2、…、s）は平文ブロックM_{uv}を鍵k_uで暗号化して得られる暗号文ブロックを示している。ここで、M_{u1}からM_{us}までのs個のブロックは同じ鍵k_uで暗号化されている。前述の鍵生成・選択装置13によって更新される鍵系列k_1、k_2、…を順にブロック暗号の鍵として用いることにより、図11の平文ブロックは複数の暗号鍵によって暗号化される。こ＊実施例1で示したような一般的なものを用いることが可能であるが、本実施例では鍵生成のアルゴリズムとして、計算量的に安全な疑似乱数系列生成アルゴリズムを用いた場合、特にその中でも2乗型疑似乱数系列を用いた場合について説明する。

【0080】2乗型疑似乱数系列とは、以下の手順で生成される疑似乱数系列b_1、b_2、…である。

［2乗型疑似乱数系列］p、qをp≡q≡3（mod 4）である素数とし、N＝p・qとして、初期値x_0（1＜x_0＜N－1なる整数）と再帰式

のように随時鍵を更新することにより、同じ鍵で暗号化される平文ブロックの数がs個になり、鍵の解析を困難にすることができる。尚、本実施例でも、暗号通信ネットワークとしては図14のものを用いる。

【0084】加入者AからBへの暗号通信は、以下の手順で行われる。ただし、前手順は実施例1と同様である。

［本発明によるデータの暗号通信手順（送信者Aに関する）］

1．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2．あらかじめ受信者Bと共有している秘密の鍵K_{AB}を通信用端末10内の鍵生成・選択装置13に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵列を生成する。

3．鍵生成・選択装置13から出力される鍵列を暗号装置11の鍵として随時更新しつつ用いデータを暗号化し、選択手段14により前手順で決定した暗号装置11から出力される暗号文を選択し、通信インタフェース12を介してBに送信する。

【0085】［本発明によるデータの暗号通信手順（受信者Bに関する）］

1．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2．あらかじめ送信者Aと共有している秘密の鍵K_{AB}を通信用端末10内の鍵生成・選択装置13に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵列を生成する。

3．通信インタフェース12を介して伝送路から暗号化データを受信し、鍵生成・選択装置13から出力される鍵列を暗号装置11の鍵として随時更新しつつ用いて、送られてきた暗号化データを復号し、選択手段14により前手順で決定した暗号装置11から出力される平文を選択する。

【0086】また、計算量的に安全な疑似乱数生成のア

ルゴリズムとして２乗型疑似乱数を用いたが、計算量的に安全な疑似乱数生成アルゴリズムであればどのようなものでも用いることができる。たとえば前記文献「暗号と情報セキュリティ」（辻井、笠原著、１９９０年発行、株式会社昭晃社、８６頁）に示されているように、ＲＳＡ暗号、離散対数、逆数暗号を用いたものも本発明の疑似乱数生成のアルゴリズムに用いることができる。また、本実施例で説明した鍵を随時更新する方法は、実施例１に基づいて説明したが、実施例１に適用できるだけでなく、実施例３、４、５に対しても適用できる。

【００８７】［実施例７］実施例１は鍵は固定の暗号方式（複数）の中からある暗号方式を選択し、実施例６は鍵は更新される暗号方式（複数）の中からある暗号方式を選択するものである。上記２つの実施例１、６のバリエーションとして本実施例では、鍵は固定の暗号方式と鍵は更新される暗号方式との間で暗号方式を選択できるようにしている。また、本実施例では、図１２に示されるような、暗号化（及び復号）を行う暗号装置１１と、通信インタフェース１２と、鍵生成・選択装置１３を備えた通信用端末１０を用いて暗号通信を行う。ここでは、説明の簡単のため暗号装置１１は１つであるとする。

【００８８】本実施例では、暗号方式としてブロック暗号を考える。さらに、そのブロック暗号を、

１．固定の鍵を用いて暗号化を行う。

２．鍵を更新しながら暗号化を行う。

のどちらの方式を使用するか暗号方式設定信号により設定できるものとする。

【００８９】鍵生成・選択装置１３は暗号方式設定信号によって制御され、「固定の鍵を用いて暗号化を行う」暗号方式で使用する場合には、鍵生成・選択装置１３は固定鍵（１つの鍵）を生成すれば処理を停止する。また、鍵を更新しながら暗号化を行う」暗号方式で使用する場合には、鍵生成・選択装置１３は鍵列（複数の鍵）を生成するために処理を繰り返し行う、という動作を行う。図１２の通信用端末１０を「固定の鍵を用いて暗号化を行う」暗号方式で使用する場合には、暗号方式設定信号により鍵生成・選択装置１３では固定鍵を生成するようにし、暗号装置１１ではその固定鍵を用いて暗号化すればよい。また、図１２の通信用端末１０を「鍵を更新しながら暗号化を行う」暗号方式で使用する場合には、暗号方式設定信号により鍵生成・選択装置１３では鍵列を生成するようにし、暗号装置１１ではその鍵列により順次鍵を更新しながら暗号化すればよい。鍵生成・選択装置１３は図２と同じ構成で動作が実施例６と同じものを用いる。暗号装置１１、通信インタフェース１２は実施例１と同じものを用いる。また、暗号通信ネットワークとしては図１４のものを用いる。

【００９０】加入者ＡからＢへの暗号通信は、実施例１と同様の手順で行われる。ただし、鍵を更新しながら暗号化を行うことを選択した場合には、データの暗号通信手順は実施例６と同様の手順で行われる。

【００９１】本実施例により、送受信者間で暗号方式について調整することができ、暗号通信の安全性を選択することができる。つまり、送信するデータの機密性に応じて暗号方式を選択できる。例えば、特に機密性の高いデータの場合には、「鍵を更新しながら暗号化を行う」暗号方式を選択し、そうでない場合には、「固定の鍵を用いて暗号化を行う」暗号方式を選択して処理を簡易にする、というようなことができる。尚、本実施例では説明の簡単のため、暗号装置１１は１つとしたが、複数の暗号装置１１を用いてもよい。その場合には、複数の暗号装置１１からの出力を選択するための選択手段１４が必要となる。

【００９２】［実施例８］本実施例は、実施例６、７で用いた鍵生成・選択装置１３の構成を少し変えた場合である。実施例６、７では、各加入者間で共有されている鍵が固定のため、「鍵を更新しながら暗号化を行う」暗号方式においても、送受信者が同じ場合には鍵生成・選択装置１３の初期値は常に同じ値となり、同じ鍵列が生成されるという問題がある。

【００９３】そこで本実施例では、送受信者が同じでも鍵生成・選択装置１３の初期値を利用する毎に変更するようにして安全性を向上させるようにしている。

【００９４】実施例６に示された鍵列生成の手順である式（７）、式（８）において、フィードバック演算により次々更新される x_{i+1} を、鍵生成・選択装置１３の内部変数と呼ぶことにする。本実施例の鍵生成・選択装置１３は、図１３に示されるように式（７）のフィードバック演算を行う処理回路１３ｈと式（８）の演算を行う処理回路１３ｉと、演算器１３ｊとから構成され、さらに式（７）の演算により更新される内部変数を読み出せる構成になっている。読み出された内部変数は、例えば実施例１で説明したような通信用端末１０に接続された携帯型記憶装置３０の保持手段３０ａに記憶される。

【００９５】実施例６、７では、鍵生成・選択装置１３へ初期値を設定するだけでデータの移動は一方向であるが、本実施例では逆方向に鍵生成・選択装置１３の内部変数の読み出しが行えるようになっている。読み出した内部変数は、次回の暗号通信に用いられる共通鍵として、今回の暗号通信に用いた共通鍵に対し置き換えが行われる。

【００９６】また、この鍵生成・選択装置１３を図１０の鍵生成・選択装置１３に置き換えることにより、鍵生成・選択装置１３の初期値を利用する毎に変更できる通信用端末１０を構成できる。

【００９７】加入者ＡからＢへの暗号通信は、実施例６、７で示した手順と同様の手順で行われる。ただし、「鍵を更新しながら暗号化を行う」暗号方式の場合には、送受信者双方に「暗号化データの復号が終了した時

の鍵生成・選択装置の内部変数の値を次回Ａ（又はＢ）と暗号通信するための新しい初期値として携帯型記憶装置の保持手段に秘密に保持する」という手順が最後に必要となる。

【００９８】上述の各実施例は、暗号方式設定信号に基づいていずれかの暗号方式を選択的に用いるように構成される。ここで、上述の暗号方式設定信号は、送信者が任意に選択してもよいし、送信されるデータの種類に応じて自動的にいずれかの暗号方式を選択するようにしてもよい。さらに、送信者が送信内容のセキュリティランクを指定する場合には、指定されたセキュリティランクに応じた強度を有する暗号方式を自動的に設定するようにしてもよい。また、上記暗号方式設定信号は、送信者Ａ、Ｂ間での動作モード、すなわち送信者Ａ、Ｂとの間の通信が、例えばＴＶ会議を行うモードや親展通信を行うモード等、に応じて自動的に暗号強度を変えるようにしてもよい。さらに、上記暗号方式の設定は、データを通信する者が優先的に設定してもよいし、両送信者から自由に設定し得るようにしてもよい。但し、暗号強度を弱くする場合には、相手方の承諾を必要とし、その承諾を得るための交渉を行う通信を行うことが好ましい。また、さらに相手側の復号能力に応じて暗号化方式を設定するようにしてもよい。

【００９９】

【発明の効果】以上説明したように、本発明によれば、暗号通信を行う送受信者の利用する通信手段に、暗号方式を選択できる選択手段を設けることにより、暗号方式を変更できるようにし、さらにその選択した暗号方式を暗号文の送信に先立って送受信者間で共有することにより、従来不可能であった暗号方式の選択を可能にし、自由度の高い暗号通信を可能にしている。

【図面の簡単な説明】

【図１】本発明の実施例１、６による通信用端末のブロック図である。

【図２】本発明の実施例１、６、７による鍵生成・選択装置のブロック図である。

【図３】本発明の実施例１による他の鍵生成・選択装置＊のブロック図である。

【図４】本発明の実施例１～８による携帯型記憶装置のブロック図である。

【図５】本発明の実施例２による通信用端末のブロック図である。

【図６】本発明の実施例３による通信用端末のブロック図である。

【図７】本発明の実施例４による通信用端末のブロック図である。

【図８】本発明の実施例４による暗号装置のブロック図である。

【図９】本発明の実施例５による暗号装置のブロック図である。

【図１０】本発明の実施例６による２乗型疑似乱数を用いた鍵生成・選択装置のブロック図である。

【図１１】本発明の実施例６による鍵更新を行う場合の暗号通信を説明するための構成図である。

【図１２】本発明の実施例７による通信用端末のブロック図である。

【図１３】本発明の実施例８による２乗型疑似乱数を用いた鍵生成・選択装置のブロック図である。

【図１４】共通鍵暗号通信ネットワークの構成図である。

【図１５】公開鍵暗号通信ネットワークの構成図である。

【図１６】共通鍵、公開鍵暗号通信ネットワークの構成図である。

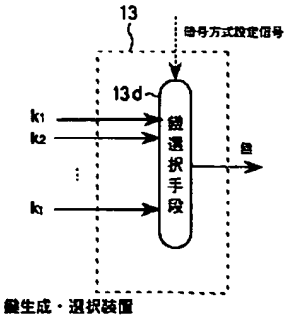
【図１７】従来の通信用端末のブロック図である。

【図１８】ＤＥＳ暗号の１段分の処理を示すブロック図である。

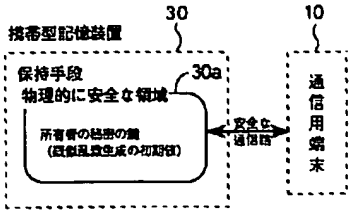
【符号の説明】

１０　通信端末
１１～２０　暗号装置
１２　通信インタフェース
１３　鍵生成・選択装置
１４　選択手段

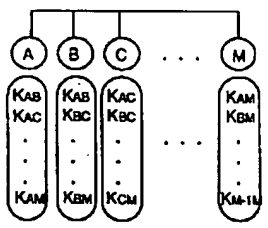
【図３】



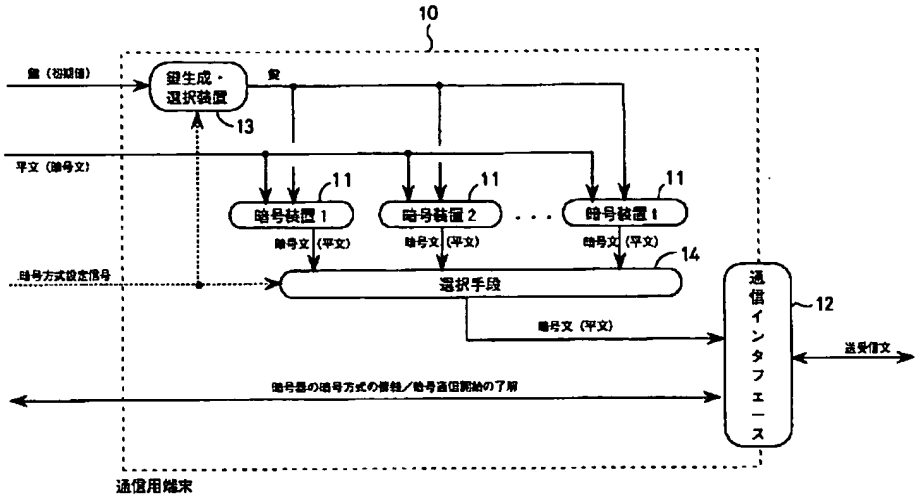
【図４】



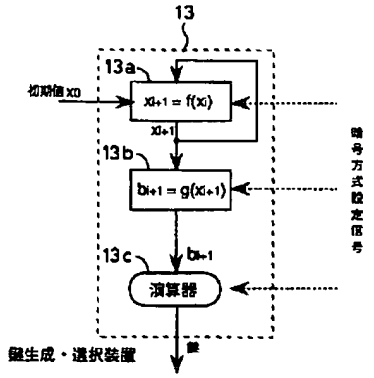
【図１４】



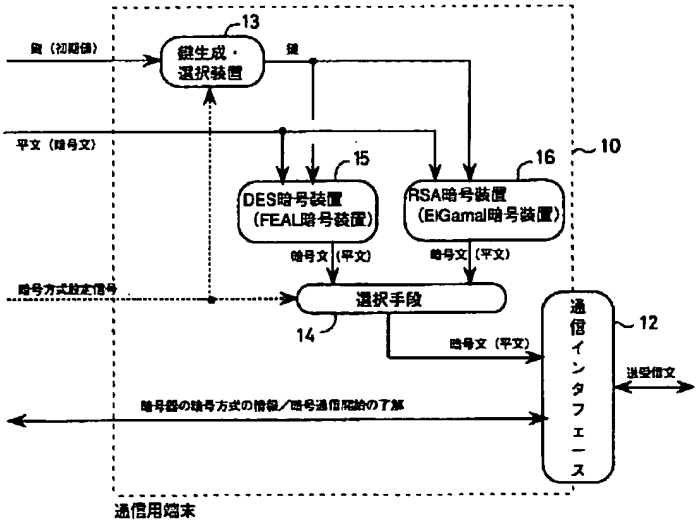
【図１】



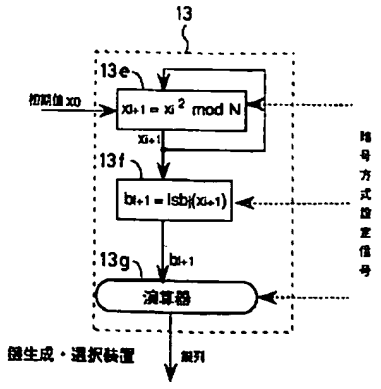
【図２】



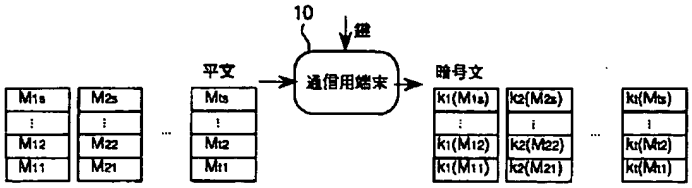
【図５】



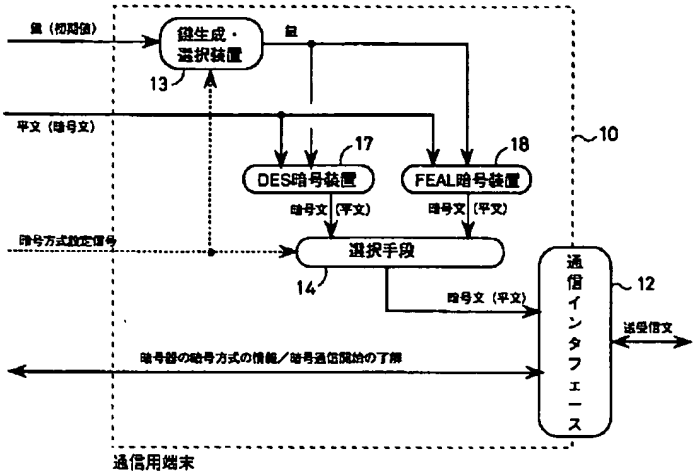
【図１０】



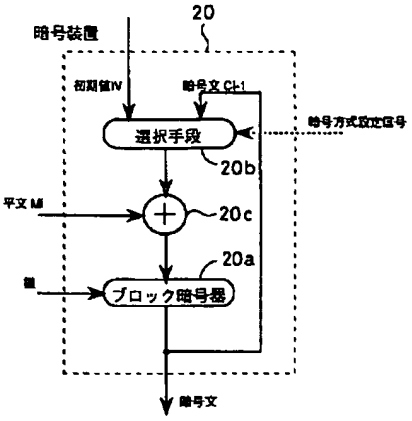
【図１１】



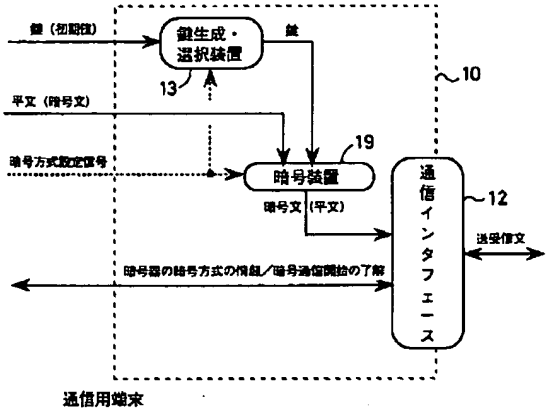
【図６】



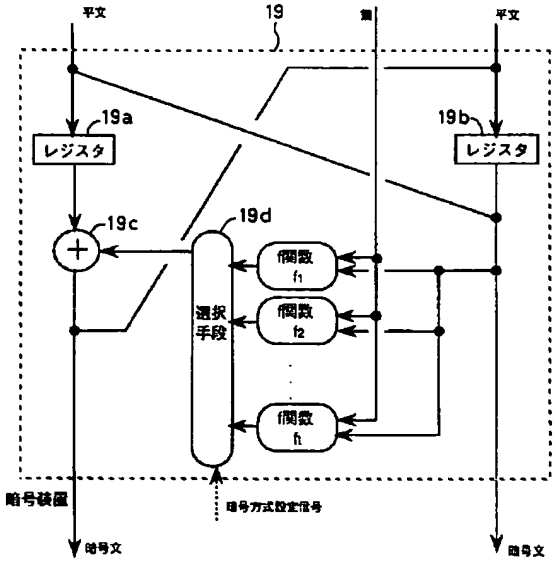
【図９】



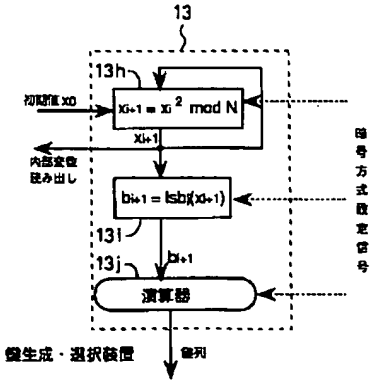
【図７】



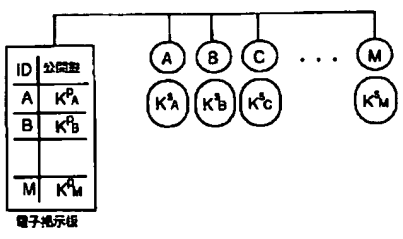
【図８】



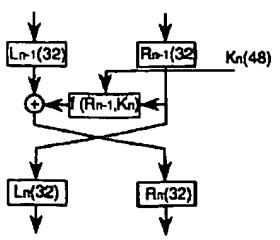
【図１３】



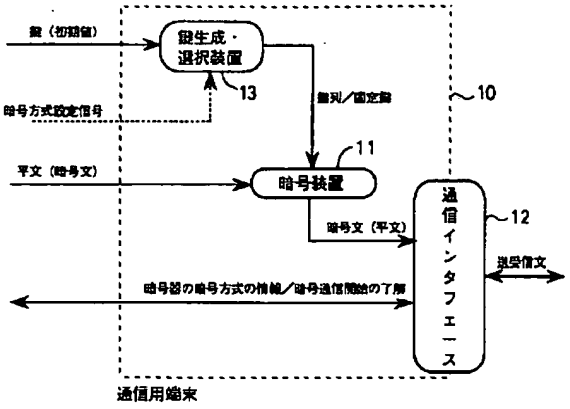
【図１５】



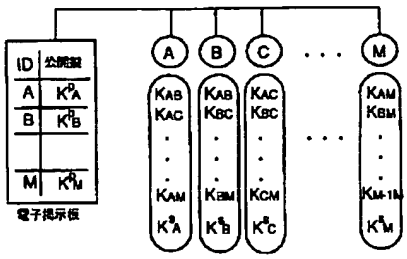
【図１８】



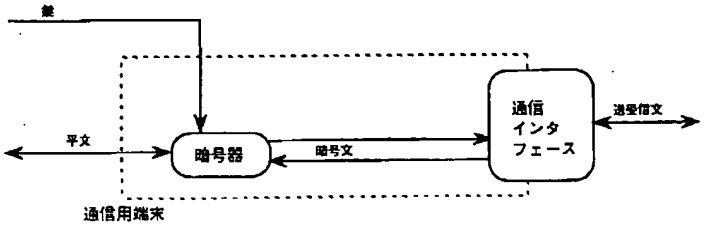
【図１２】


鍵（初期値）
鍵生成・選択装置
13
暗号方式設定信号
暗号鍵/固定鍵
10
11
平文（暗号文）
暗号装置
暗号文（平文）
12
通信インタフェース
送受信文
暗号器の暗号方式の情報/暗号通信開始の了解
通信用端末

【図１６】


ID
公開鍵
A
B
M
電子掲示板
A
B
C
M

【図１７】


鍵
平文
暗号器
暗号文
通信インタフェース
送受信文
通信用端末